Manuel de l'utilisateur du module HP BladeSystem Onboard Administrator

Résumé
Ce manuel fournit des informations sur la configuration initiale et le fonctionnement du module HP Blade System Onboard Administrator. Il couvre également l'utilisation de l'interface graphique utilisateur Onboard Administrator et l'écran Insight Display du boîtier. Les informations contenues dans ce manuel s'appliquent à la version 4.50 (ou ultérieure) du module HP Blade System Onboard Administrator.

© Copyright 2006, 2015 Hewlett-Packard Development Company, L.P.

Les informations contenues dans ce document pourront faire l'objet de modifications sans préavis. Les garanties relatives aux produits et services HP sont exclusivement définies dans les déclarations de garantie limitée qui accompagnent ces produits et services. Aucun terme de ce document ne peut être interprété comme constituant une garantie supplémentaire. HP ne pourra être tenue responsable des éventuelles erreurs ou omissions de nature technique ou rédactionnelle qui pourraient subsister dans le présent document.

Des liens vers des sites Web tiers vous mènent hors du site Web HP. HP n'exerce aucun contrôle sur ces liens et n'est pas responsable des informations en dehors de HP.com.

Microsoft®, Windows®, Windows Vista®, Windows® XP, Windows® 7 et Windows Server® sont des marques déposées aux États-Unis du groupe de sociétés Microsoft. Google™ est une marque déposée de Google Inc. Java est une marque déposée d'Oracle et/ou de ses filiales. Red Hat® est une marque déposée de Red Hat, Inc. aux États-Unis et dans d'autres pays. UNIX® est une marque déposée de The Open Group.

Référence : 695522-059a

octobre 2015

Édition : 24

Sommaire

1 Introduction 1

Présentation 1

Exigences d'accès 3

Présentation du module Onboard Administrator 4

Interfaces 6

Authentification du module Onboard Administrator 7

Première exécution du module Onboard Administrator 8

Connexion à l'interface du module Onboard Administrator 9

Récupération flash d'urgence 11

Exécution de l'assistant d'installation 12

Utilisation de l'aide en ligne 13

Modification de la configuration du boîtier et des périphériques 14

Récupération du mot de passe administrateur 14

Considérations de sécurité 15

Présentation de l'architecture de réseau BladeSystem 15

Pratiques d'excellence de sécurité recommandées 15

Ports réseau 17

Fonctionnalités de sécurité cryptographique et valeurs par défaut 17

2 Installation matérielle des boîtiers HP BladeSystem c3000/c7000 23

Installation de modules Onboard Administrator 23

Câblage du module Onboard Administrator 23

3 HP BladeSystem Insight Display 26

Composants de l'écran Insight Display 2 pouces du modèle HP BladeSystem c7000 26

Composants de l'écran Insight Display 3 pouces des modèles HP BladeSystem c3000 et c7000 27

Présentation du module Insight Display 27

Accès à l'écran HP BladeSystem c3000 Insight Display 28

Exécution de l'installation du module Insight Display 29

Navigation dans le module Insight Display 35

Écran Health Summary 37

Écran Enclosure Settings 38

Écran Enclosure Info 39

Écran Blade and Port Info 39

Écran Turn Enclosure UID On/Off 41

Écran View User Note 42

Écran Chat Mode 42
Écran USB Menu 43
Écran KVM Menu 46
Erreurs du module Insight Display 46
Erreurs d'alimentation 47
Erreurs de refroidissement 47
Erreurs d'emplacement 47
Erreurs de configuration 47
Erreur de panne de périphérique 48

4 Boîtier KVM 49
Fonctionnalités 49

5 Assistant First Time Setup 54
Avant de commencer 54
Connexion au module Onboard Administrator 54
Préférences de l'utilisateur 55
FIPS 56
Écran Enclosure Selection 58
Écran Configuration Management 59
Écran Rack and Enclosure Settings 60
Écran Administrator Account Setup 62
Écran Local User Accounts 63
Adressage IP des baies de boîtiers 64
Écran Directory Group Configuration 73
Écran Directory Settings 75
Écran Onboard Administrator Network Settings 78
Écran Enclosure SNMP Settings 85
Écran Power Management 86
Finalisation 94

6 Navigation dans le module Onboard Administrator 96
Présentation de la navigation 96
Arborescence 96
Navigation dans la vue graphique 99

7 Vue du rack 102
Écran Rack Overview 102
Modes de topologie 104
Onglet Rack Topology 105

Onglet Rack Power and Thermal 106
Écran Rack Firmware 108

8 Configuration des boîtiers HP BladeSystem et des périphériques de boîtier 112
Affichage des écrans d'état 112
Paramètres du boîtier 113
Sélection de boîtiers 113
Écran Enclosure Information 113
AlertMail 117
Onglets de baies de périphériques de séquence d'alimentation de périphériques 120
Onglet de baies d'interconnexion de séquence d'alimentation de périphériques 123
Date et heure 123
Paramètres TCP/IP du boîtier 126
Onglet IPv4 Settings 126
Onglet IPv6 Settings 129
Onglet NIC Options 135
Onglet Advanced Settings 135
Accès réseau 136
Onglet Trusted Hosts 137
Onglet Anonymous Data 138
Onglet FIPS 139
Onglet Login Banner 141
Link Loss Failover 141
Paramètres SNMP 142
Adressage IP des baies de boîtiers 147
Adressage EBIPA pour IPv4 150
Adressage EBIPA pour IPv6 153
Résumé des périphériques 157
Actif à Standby 160
Lecteur de DVD 160
Installation et configuration interactives du lecteur de DVD/CD-ROM 163
Déploiement sans assistance de système d'exploitation 169
Accès ad-hoc au support basé sur DVD pour installation d'application ou importation de données 175
Mise à jour de microprogramme de lame avec HP Smart Update Manager ... 175
Configuration VLAN 175
Paramètres VLAN 177
Ajout, édition et suppression de réseaux VLAN 179
Configuration de périphériques 180
Active Health System 182

Inscription à Insight Remote Support 183
Événements de service Insight Remote Support 190
Collectes de données Insight Remote Support 192
Informations de collecte de données 192
Administration de certificat de Remote Support 193
Onglet Support Certificate Administration Upload de Remote Support 194
Enclosure Firmware Management 195
Détection manuelle 202
Mise à jour manuelle 203
Journal Enclosure Firmware Management 203
Mises à jour d'état 204
Gestion de boîtiers 206
Mise hors tension du boîtier 206
Liaison de boîtiers 206
Gestion de plusieurs boîtiers 207
Module Onboard Administrator actif 207
Écran Active Onboard Administrator 207
Onglet Virtual Buttons du module Onboard Administrator actif 209
Onglet USB du module Onboard Administrator actif 210
Écran TCP/IP Settings du module Onboard Administrator actif 211
Onglet d'informations d'administration de certificat 215
Onglet Certificate Request 217
Onglet Certificate Upload 220
Mise à jour du microprogramme 221
Mise à niveau de modules Onboard Administrator dans un boîtier HP BladeSystem 224
Onglet Language Pack 225
Journal système 227
Onglet Log Options 227
Module Onboard Administrator en mode Standby 228
Écran Standby Onboard Administrator 228
Onglet Virtual Buttons du module Onboard Administrator en mode Standby 229
Paramètres TCP/IP pour module OA en Standby, vu du module OA actif 230
Onglet Standby Onboard Administrator Certificate Administration Information 232
Onglet Standby Certificate Request 234
Onglet Standby Certificate Upload 236
Journal système pour module Onboard Administrator en Standby 236
Standby à Actif 236
Baies de périphérique 237
Baies de périphérique 237
Onglet Device Bay Status 240

Onglet Server Blade Information 246
Onglet Server Blade Virtual Devices 249
Onglet Boot Options 251
Onglet IML Log 253
Écran iLO 254
Onglet iLO Event Log 256
Mappage de ports 256
Vue graphique de mappage de ports de baie de périphérique pour boîtier c3000 258
Tableau de mappage de ports de baie de périphérique pour boîtier c3000 ... 262
Vue graphique de mappage de ports de baie de périphérique pour boîtier c7000 266
Tableau de mappage de ports de baie de périphérique pour boîtier c7000 ... 271
Microprogrammes 274
Initiation d'une mise à jour ou détection manuelle 276
Journaux de gestion des microprogrammes 280
Affichage des versions des microprogrammes 282
Variations de versions de microprogrammes 284
Lames de stockage 284
Informations de lame d'extension E/S 289
Onglet de périphériques virtuels de lame d'extension E/S 290
Onglet d'informations de lame d'extension E/S 291
Baies d'interconnexion 291
Écran Interconnect Bay Summary 291
Écran Interconnect Bay 293
Onglet Interconnect Bay Information 296
Boutons virtuels de la baie d'interconnexion 298
Écran Interconnect Bay Port Mapping 298
Gestion de l'alimentation de boîtier 300
Planification de la gestion de l'alimentation 300
Écran Power and Thermal 300
Gestion de l'alimentation 301
Écran Enclosure Power Meter 310
Onglet Graphical View 311
Onglet Table View 312
Allocation de l'alimentation du boîtier 314
Récapitulatif de la puissance du boîtier 315
Écran Power Subsystem 316
Informations d'alimentation 317
Gestion des ventilateurs et de la ventilation 318
Zones de ventilateur 318

Sous-système thermique 320
Règles d'emplacement des ventilateurs du boîtier c7000 324
Règles d'emplacement des ventilateurs du boîtier c3000 325
Gestion des utilisateurs 326
Authentification des utilisateurs 326
Rôles et niveaux de privilège utilisateur 326
Comptes utilisateur basés sur les rôles 327
Utilisateurs locaux 328
Ajout d'un utilisateur local 329
Modification de l'utilisateur local 330
Modification des informations de certificat des utilisateurs locaux 333
Paramètres de mot de passe 333
Écran Directory Settings 334
Onglet Directory Certificate Information 337
Téléchargement d'un certificat 337
Onglet Directory Certificate Upload 338
Onglet Directory Test Settings 339
Groupes d'annuaires 341
Ajout d'un groupe LDAP 342
Modification d'un groupe LDAP 345
Administration SSH 348
Versions SSH et SSL prises en charge 348
Intégration de HP SSO 349
Authentification à deux facteurs 350
Onglet Certificate Information de l'authentification à deux facteurs 351
Onglet Certificate Upload de l'authentification à deux facteurs 351
Signed In Users 351
Onglet Session Options 352
Insight Display 353
Virtual Connect Manager 353
Intégration iLO 354
Dépendances IP du réseau de supervision 354

9 Utilisation de l'interface de ligne de commande 356
Présentation de la ligne de commande 356
Installation du module Onboard Administrator à l'aide de l'interface CLI 356
Signaux de broche du connecteur série RS232 du module Onboard Administrator 358
Utilisation de la connexion du port du service 358
Utilisation de scripts de configuration 359
Scripts de configuration 359
Réinitialisation des valeurs usine par défaut 361

10 Prise en charge de lame de serveur HP Integrity i2 363
Prise en charge mise à jour pour lames de serveur HP Integrity BL860c i2, BL870c i2 et BL890c i2 363
Modification de vue d'arborescence et de vue graphique pour lames de serveur HP Integrity i2 363
Modification de mappage de ports pour lames de serveur HP Integrity i2 365
Modifications de lames partenaires pour lames de serveur HP Integrity i2 365

11 Résolution des problèmes 366
Messages d'erreur du module Onboard Administrator 366
Paramètres usine par défaut du module Onboard Administrator 389
Interruptions SNMP du module Onboard Administrator 389
Problèmes connus liés au navigateur 390
Problèmes de réseau connus 392
Problèmes connus divers 393

12 Activation de l'authentification de services d'annuaire LDAP auprès de Microsoft Active Directory 396
Services de certificat 396
Préparation de l'annuaire 396
Téléchargement du certificat de contrôleur de domaine (facultatif) 397
Création de groupes d'annuaire 400
Test de la solution de connexion à l'annuaire 401
Résolution des problèmes LDAP sur Onboard Administrator 402

13 Création d'autorités de certification et configuration de l'autorisation à deux facteurs pour comptes de groupe LDAP et d'utilisateur local 404
Introduction 404
Configuration des répertoires 407
Création d'un répertoire pour représenter chaque autorité de certification et chaque utilisateur 407
Modification et stockage d'un fichier de configuration OpenSSL dans chaque répertoire d'autorité de certification 408
Modification des répertoires par défaut 408
Création d'une autorité de certification racine 408
Copie du fichier de configuration OpenSSL dans le répertoire de l'autorité de certification racine 408
Création du certificat et de la clé privée 408
Création d'un fichier PEM combiné de certificat et de clé privée 410
Création d'autorités de certification subordonnées 410
Création de répertoires pour l'autorité de certification subordonnée 410
Fourniture d'informations de certificat x509 410
Génération d'une CSR et d'une nouvelle clé de serveur 411

Signature de la CSR level1CA avec la clé rootCA 412
Création de clés d'utilisateur et de CSR 412
Création d'un répertoire pour la clé utilisateur et la base de données de CSR 412
Fourniture d'informations de certificat utilisateur x509 413
Génération d'une CSR d'utilisateur et d'une nouvelle clé de serveur 413
Signature de la CSR d'utilisateur avec la clé level1CA 413
Vérification de certificats 416
Stockage d'un certificat utilisateur sur une carte à puce ou un navigateur 417
Configuration du module Onboard Administrator pour l'authentification à deux facteurs avec comptes locaux 419
Établissement d'un plan de récupération du module Onboard Administrator 419
Récupération via l'écran Insight Display et la clé USB 419
Récupération via la console série 420
Configuration de l'expiration de la session Onboard Administrator 420
Installation de la chaîne d'autorités de certification pour authentification à deux facteurs 421
Commandes CLI pour administration de certificats 424
Configuration du proxy HTTP 424
Installation de certificats utilisateur sur le compte administrateur local 424
Activation de l'authentification à deux facteurs 426
Connexion à l'interface Web Onboard Administrator à l'aide de l'authentification à deux facteurs 427
Authentification TFA+LDAP 427
Fonctionnement de l'authentification TFA+LDAP 428
Activation de l'authentification TFA+LDAP 428
Méthodes de spécification du champ d'objet sur une CSR 428
Résolution des problèmes d'authentification TFA et LDAP 429
Exemples de l'interface CLI pour configuration d'un compte utilisateur et de certificats 430
Informations sur les autorités de certification et les certificats disponibles à partir du Web 432

14 Paramètres des fuseaux horaires 433
Paramètres de fuseaux horaires universels 433
Paramètres de fuseaux horaires de la zone Afrique 433
Paramètres de fuseaux horaires de la zone Amérique 434
Paramètres de fuseaux horaires de la zone Asie 436
Paramètres de fuseaux horaires de la zone Océanie 437
Paramètres de fuseaux horaires de la zone Europe 438
Paramètres de fuseaux horaires de la zone polaire 438

15 Assistance et autres ressources 440
Avant de contacter HP 440

Informations de contact HP 440
Informations complémentaires 441

16 Acronymes et abréviations 442

17 Commentaires sur la documentation 446

Index 447

1 Introduction

Présentation

HP BladeSystem Onboard Administrator est la base du processeur de supervision du boîtier, du sous-système et du microprogramme utilisée pour prendre en charge le boîtier HP BladeSystem c-Class et tous les périphériques gérés présents dans le boîtier.

Le module Onboard Administrator fournit un point d'entrée unique pour l'exécution des principales tâches de supervision des lames de serveur ou commutateurs du boîtier. Le module Onboard Administrator réalise les étapes de configuration du boîtier, active la gestion et la configuration d'exécution des composants du boîtier et vous informe des problèmes au sein du boîtier par courrier électronique, SNMP ou Insight Display.

HP vous recommande de lire le Manuel de l'utilisateur du boîtier HP BladeSystem c3000 ou c7000 pour obtenir des informations spécifiques sur le boîtier avant de continuer avec l'installation du module Onboard Administrator.

Le module HP BladeSystem Onboard Administrator fournit plusieurs fonctionnalités conçues pour simplifier la supervision de lames c-Class et des interconnexions. Les boîtiers BladeSystem c3000 et c7000 peuvent être configurés avec des modules Onboard Administrator redondants pour fournir une facilité de gestion ininterrompue sur l'intégralité du boîtier et des lames en cas de panne d'un module Onboard Administrator unique. Le tableau suivant indique quelle fonctionnalité du module Onboard Administrator est améliorée lorsque le boîtier contient des modules Onboard Administrator redondants. Pour un boîtier doté d'un module Onboard Administrator unique, le tableau indique le comportement du boîtier si le module Onboard Administrator est défectueux ou est retiré. La fonctionnalité Enclosure Dynamic Power Capping (Plafond d'alimentation dynamique du boîtier), introduite avec la version 2.31 du microprogramme Onboard Administrator, est uniquement disponible dans les boîtiers HP BladeSystem avec des modules Onboard Administrator redondants installés.

Avantages de l'utilisation d'un module Onboard Administrator redondant par rapport à un module Onboard Administrator unique

Fonctionnalité du module Onboard Administrator	Module Onboard Administrator unique dans le boîtier	Le module Onboard Administrator unique est en panne ou a été retiré	Module Onboard Administrator redondant dans le boîtier
Allocation et contrôle de l'alimentation pour toutes les lames et interconnexions	Oui. Aucun plafond d'alimentation dynamique du boîtier car ceci nécessite des modules Onboard Administrator redondants.	Non. Les sources d'alimentation fournissent l'alimentation à toutes les lames et interconnexions. Aucune demande de mise sous tension ne peut être faite pour les lames ou les interconnexions.	Oui. Contrôle intégral, y compris la prise en charge en cas de panne sur l'un ou l'autre module Onboard Administrator. Enclosure Dynamic Power Capping nécessite des modules Onboard Administrator redondants.
Refroidissement pour toutes les lames et interconnexions.	Oui. Contrôle intégral.	Non. Tous les ventilateurs de boîtier vont utiliser une vitesse plus élevée non gérée pour empêcher les lames et les interconnexions de surchauffer.	Oui. Contrôle intégral, y compris la prise en charge en cas de panne sur l'un ou l'autre module Onboard Administrator.

Fonctionnalité du module Onboard Administrator	Module Onboard Administrator unique dans le boîtier	Le module Onboard Administrator unique est en panne ou a été retiré	Module Onboard Administrator redondant dans le boîtier
Enclosure Bay IP Addressing (EBIPA)	Oui. Contrôle intégral.	Non. Les adresses IP EBIPA seront perdues une fois le délai d'attente dépassé.	Oui. Contrôle intégral, y compris la prise en charge en cas de panne sur l'un ou l'autre module Onboard Administrator.
Communications Ethernet au module Onboard Administrator, serveur iLO, processeurs de supervision d'interconnexion tels que Virtuel Connect utilisant le port de supervision du module Onboard Administrator/iLO	Oui. Contrôle intégral.	Non. Communications de supervision Ethernet, y compris le trafic de supervision interne tel que le Virtual Connect Manager vers d'autres modules VC dans le boîtier.	Oui. Contrôle intégral, y compris la prise en charge en cas de panne sur l'un ou l'autre module Onboard Administrator.
Informations et état d'intégrité concernant les lames, interconnexions, ventilateurs, alimentations, modules Onboard Administrator et boîtier via l'interface utilisateur de module Onboard Administrator ou CLI, des messages d'alerte ou SNMP	Oui. Contrôle intégral.	Aucune information disponible du module Onboard Administrator ni aucune information hors bande disponible de VCM ou iLO sur tout serveur.	Oui. Contrôle intégral, y compris la prise en charge en cas de panne sur l'un ou l'autre module Onboard Administrator.
Insight Display	Oui. Contrôle intégral.	Non.	Oui. Contrôle intégral, y compris la prise en charge en cas de panne sur l'un ou l'autre module Onboard Administrator.
DVD du boîtier (nécessite l'option c3000 DVD, le lecteur de DVD USB externe ou la clé USB)	Oui. Contrôle intégral.	Non.	Oui. Contrôle intégral, y compris la prise en charge en cas de panne sur l'un ou l'autre module Onboard Administrator.
Option KVM de boîtier (nécessite l'option c3000 KVM ou le module Onboard Administrator avec le connecteur VGA)	Oui. Contrôle intégral.	Non.	Oui. Contrôle intégral. Pour le boîtier HP c3000, nécessite à la fois l'option c3000 KVM et l'option Onboard Administrator redondante. Pour le boîtier HP c7000, nécessite deux des modules Onboard Administrator les plus récents avec le connecteur VGA.

Paramètres Onboard Administrator stockés et remplacement de module

Modèle du boîtier	Module Onboard Administrator unique dans le boîtier	Module Onboard Administrator redondant (même type de remplacement installé)[1]	Module Onboard Administrator redondant (type de remplacement différent installé)[1]
c3000	Tous les paramètres du boîtier sont perdus lorsqu'un module unique est retiré et doivent être restaurés manuellement via l'écran Insight Display et la clé USB, l'interface utilisateur graphique ou la ligne de commande.	Tous les paramètres du boîtier sont conservés sur le module restant et ces paramètres sont synchronisés sur le module remplacé en cas de discordance des versions de microprogramme.[2]	Lors du changement du module Onboard Administrator c3000 non-redondant en module Onboard Administrator redondant avec DDR2, les paramètres du boîtier doivent être restaurés manuellement via l'écran Insight Display et la clé USB, l'interface utilisateur graphique ou la ligne de commande.
c7000	Tous les paramètres du boîtier sont perdus lorsqu'un module unique est retiré et doivent être restaurés manuellement via l'écran Insight Display et la clé USB, l'interface utilisateur graphique ou la ligne de commande.	Tous les paramètres du boîtier sont conservés sur le module restant et ces paramètres sont synchronisés sur le module remplacé en cas de discordance des versions de microprogramme.[2]	Tous les paramètres du boîtier sont conservés sur le module restant et ces paramètres sont synchronisés sur le module remplacé en cas de discordance des versions de microprogramme.[2]

[1] Lorsqu'un module Onboard Administrator redondant est retiré, le module restant devient immédiatement le module Onboard Administrator actif.

[2] En cas de discordance des versions de microprogramme Onboard Administrator, les paramètres ne sont pas automatiquement synchronisés. Synchronisez le microprogramme via l'écran Insight Display et la clé USB, l'interface utilisateur graphique ou la ligne de commande, et les paramètres sont automatiquement synchronisés sur le module Onboard Administrator remplacé.

Exigences d'accès

Pour accéder à l'interface Web du module HP BladeSystem Onboard Administrator, vous devez disposer de l'adresse IP du module Onboard Administrator et d'un navigateur Web compatible. Vous devez accéder à l'application par HTTPS (paquets HTTP échangés sur une session cryptée en SSL/TLS).

L'interface Web du module HP BladeSystem Onboard Administrator nécessite un navigateur compatible XSLT qui prend en charge JavaScript 1.3 ou équivalent.

Pour obtenir la liste des navigateurs pris en charge pour une utilisation avec le module Onboard Administrator, consultez la dernière version des notes de publication du module Onboard Administrator.

Avant d'exécuter le navigateur Web, vous devez activer les paramètres de navigateur suivants :

- ActiveX (pour Microsoft® Internet Explorer)
- Cookies
- JavaScript

Si un message vous avertit que votre navigateur ne dispose pas de la fonctionnalité requise, vérifiez que les paramètres du navigateur correspondent aux exigences précédentes et consultez la section « Récupération du mot de passe administrateur » (Récupération du mot de passe administrateur à la page 14).

Si vous utilisez un module de langue installé avec l'interface Onboard Administrator et que le navigateur n'affiche pas tous les caractères correctement, assurez-vous que le système d'exploitation dispose de la prise en charge installée de la langue correspondante.

Pour accéder à l'interface CLI du module HP BladeSystem Onboard Administrator, utilisez l'adresse IP du module HP BladeSystem Onboard Administrator et un terminal ou une application depuis un terminal. Pour accéder à l'interface CLI, vous devez utiliser Telnet ou SSH selon le protocole activé.

Les ports suivants sont utilisés pour accéder et surveiller le module Onboard Administrator.

Protocole	Port entrant	Port sortant
SSH	22	—
Telnet	23	—
SMTP	—	25
Accès au navigateur	80	80
Accès crypté de navigateur	443	443
Lecture/Commande SNMP	161	—
Interruptions SNMP	—	162
LDAP SSL	—	636
Catalogue mondial LDAP	—	3269
Authentification directe des services de terminaux de PC à iLO	3389	—
Console distante iLO	17790	—
Supports virtuels de PC à iLO	17988	—
Fonctionnalité Syslog à distance	—	514

Vous pouvez modifier les numéros de port des journaux système LDAP et Remote.

Si un protocole est désactivé, les ports correspondants sont également désactivés.

Pour utiliser EDPC, le microprogramme iLO version 1.70 ou ultérieure est requis.

REMARQUE : Le module Onboard Administrator prend en charge plusieurs sessions de connexion simultanées, soit par l'interface Web du Onboard Administrator, soit par l'interface CLI, excepté pour les utilisateurs de LDAP/Active Directory où une seule session de connexion est autorisée par utilisateur.

Présentation du module Onboard Administrator

La supervision d'un boîtier c-Class implique plusieurs fonctions :

- Détection de l'insertion et du retrait de composants
- Identification des composants, y compris connectivité requise
- Supervision de l'alimentation et du refroidissement
- Contrôle des composants, y compris télécommande et consoles distantes

Détection de l'insertion et du retrait de composants

Le module Onboard Administrator fournit un contrôle des composants dans les boîtiers c-Class. La supervision des composants commence une fois un composant détecté et identifié. Le module Onboard Administrator détecte les composants dans les boîtiers BladeSystem c-Class au travers de signaux de présence sur chaque baie. Lorsque vous insérez un composant dans une baie, le module Onboard Administrator le reconnaît et l'identifie immédiatement. Lorsque vous retirez un composant d'une baie, le module Onboard Administrator supprime les informations relatives à celui-ci.

Identification des composants

Pour identifier un composant, le module Onboard Administrator lit une EEPROM FRU qui contient des informations usine spécifiques sur celui-ci, telles que nom du produit, référence et numéro de série. Toutes les EEPROM FRU dans les boîtiers c-Class sont mises sous tension, même si le composant est désactivé. Par conséquent, le module Onboard Administrator peut identifier le composant avant d'accorder l'alimentation. Pour les périphériques tels que les ventilateurs, les alimentations et les écrans Insight Display, le module Onboard Administrator lit directement les EEPROM FRU. Le module Onboard Administrator accède aux EEPROM FRU de lame de serveur via des processeurs de supervision iLO.

- Les lames de serveur contiennent plusieurs EEPROM FRU : une sur la carte du serveur, qui contient des informations sur le serveur et sur la carte réseau intégrée, et une sur chaque carte mezzanine en option installée.
- Les options de contrôle de lame de serveur incluent la connexion automatique à l'interface Web iLO et aux consoles de serveur distant, un contrôle d'alimentation virtuelle, ainsi qu'une commande d'ordre de démarrage. Les options de contrôle de lame de serveur incluent également des informations étendues concernant le matériel du serveur, notamment versions de microprogramme de BIOS et iLO, nom du serveur, ID de port de carte réseau et carte en option, ainsi que mappage de ports.
- Le module Onboard Administrator fournit des informations de mappage de ports pour chaque lame de serveur et module d'interconnexion dans le boîtier.

Les informations FRU de carte réseau et de carte mezzanine en option indiquent au module Onboard Administrator le type d'interconnexion requis par chaque serveur. Avant que l'alimentation ne soit fournie à une lame de serveur, le module Onboard Administrator compare ces informations aux EEPROM FRU sur les modules d'interconnexion installés pour vérifier les erreurs de saisie électronique. Dans le cas de modules d'interconnexion, le module Onboard Administrator fournit un contrôle d'alimentation virtuelle, des consoles série dédiées et des connexions Ethernet de supervision.

Un indicateur de progression à 16 étapes apparaît lorsque le module Active Onboard Administrator démarre. Certaines étapes peuvent durer plusieurs minutes, en fonction du nombre et des types de lames, cartes mezzanine et interconnexions.

Supervision de l'alimentation et du refroidissement

Les tâches les plus importantes du module Onboard Administrator sont la supervision de l'alimentation et du refroidissement. Le module Onboard Administrator peut contrôler à distance l'état d'alimentation de tous les composants dans les boîtiers BladeSystem c-Class. Pour les composants dans les baies de périphériques à l'avant de chaque boîtier, le module Onboard Administrator communique avec iLO pour contrôler les serveurs, et avec un microcontrôleur pour contrôler des options telles que les lames de stockage. Un microcontrôleur distinct contrôle l'alimentation des modules d'interconnexion.

Une fois les composants alimentés, le module Onboard Administrator démarre une supervision thermique à l'aide de la fonction Thermal Logic. La fonction Thermal Logic des boîtiers BladeSystem c-Class minimise la consommation électrique du sous-système de ventilateurs en lisant les capteurs de température répartis dans tout le boîtier. La fonction Thermal Logic modifie ensuite la vitesse des

ventilateurs dans les différentes zones du boîtier pour minimiser la consommation électrique et maximiser l'efficacité du refroidissement.

Contrôle des composants

Le module Onboard Administrator utilise des interfaces de supervision incorporées pour fournir des informations détaillées, y compris sur l'état d'intégrité pour toutes les baies dans le boîtier, notamment les signaux de détection de présence dans chaque baie, et sur les contrôleurs i2c, série, USB et Ethernet. Il propose également des informations sur les versions de microprogramme pour la plupart des composants du boîtier et peut être utilisé pour mettre à jour ces composants.

Interfaces

Chaque boîtier c-Class comporte plusieurs interfaces externes de supervision qui connectent l'utilisateur au module Onboard Administrator. La prise RJ-45 Ethernet est l'interface primaire. Cette interface fournit un accès réseau au Onboard Administrator et à l'interface de gestion sur toutes les lames de serveur (iLO), les lames de stockage (TBM) et les modules d'interconnexion.

Un port série sur le module Onboard Administrator fournit un accès hors bande complet par l'interface CLI au module Onboard Administrator et est utilisé pour la récupération flash du microprogramme Onboard Administrator.

Les ports USB sur le module Onboard Administrator sont utilisés pour connecter des lecteurs de DVD externes de manière à prendre en charge la fonctionnalité DVD du boîtier. De plus, vous pouvez commander un lecteur de DVD interne facultatif pour le boîtier c3000. Le port USB sur le module Onboard Administrator peut avoir un autocollant sur le port indiquant que ce dernier est réservé pour une utilisation ultérieure. Pour utiliser le port USB avec la version 2.00 ou ultérieure du microprogramme du module Onboard Administrator, retirez l'autocollant.

Tous les boîtiers c-Class prennent en charge deux connecteurs de liaison de boîtier qui fournissent des communications privées entre les boîtiers reliés par un câble CAT5. Le connecteur « haut » de liaison de boîtier fournit un port de service de boîtier qui permet aux utilisateurs de connecter temporairement un ordinateur portable à tout module Onboard Administrator de boîtier lié pour des diagnostics locaux et un débogage.

L'option KVM Module (Module KVM) pour le boîtier c3000 se branche sur la baie arrière adjacente au module d'interconnexion 1 et fournit un connecteur VGA et deux connecteurs USB supplémentaires pour le boîtier c3000. Ce module KVM active la fonction KVM du boîtier pour le boîtier c3000. Le connecteur VGA joint est relié à un moniteur VGA externe, ainsi qu'à un clavier et à une souris USB externes pour fournir l'accès à toutes les consoles vidéo du serveur ou à l'interface CLI du module Onboard Administrator ou encore au module Insight Display.

Le nouveau module Onboard Administrator c7000 avec KVM ajoute un connecteur VGA au module Onboard Administrator c7000, en activant la fonction KVM du boîtier pour le boîtier c7000. Le module Onboard Administrator c7000 actif avec KVM fournit les mêmes fonctions KVM du boîtier que le module KVM c3000 facultatif. Un concentrateur USB externe (non fourni) doit être utilisé pour connecter un lecteur de DVD USB en même temps que le KVM USB pour clavier et souris de manière à disposer simultanément des fonctionnalités KVM du boîtier et DVD du boîtier. Le module Onboard Administrator en mode Standby avec KVM fournit seulement l'accès à la connexion à l'interface CLI du module Onboard Administrator. Ceci permet à l'utilisateur connecté de prendre le contrôle.

Chaque boîtier c-Class comprend un module Insight Display intégré sur le devant du boîtier qui fournit l'état et des informations sur toutes les baies dans un boîtier c-Class, ainsi que des informations de diagnostic si le module Onboard Administrator détecte un problème dans le boîtier. Le module Insight Display configure des paramètres clés dans le module Onboard Administrator, notamment l'adresse IP de ce dernier.

Authentification du module Onboard Administrator

La sécurité est assurée pour toutes les interfaces utilisateur de module Onboard Administrator via authentification utilisateur. Les comptes utilisateurs créés dans le module Onboard Administrator se voient affecter l'un des trois niveaux de privilège et octroyer l'accès aux baies de composants au niveau de privilège spécifié. Le module Onboard Administrator enregistre les mots de passe pour les comptes d'utilisateurs locaux et peut être configuré pour utiliser l'authentification LDAP pour les comptes de groupes d'utilisateurs. Le module Insight Display peut être protégé par un numéro d'identification personnelle LCD ou être complètement désactivé. Un code PIN LCD protège contre l'accès non autorisé à Insight Display et Enclosure KVM. L'utilisation du module KVM pour accéder aux consoles de serveur est protégée à l'aide du nom d'utilisateur/mot de passe sur le système d'exploitation du serveur.

REMARQUE : Le module Onboard Administrator ne prend pas en charge OpenLDAP.

Comptes utilisateur basés sur les rôles

Le module Onboard Administrator fournit des comptes utilisateur configurables permettant de définir clairement plusieurs rôles d'administrateur de type serveur, réseau local et réseau SAN. Les comptes utilisateur sont configurés avec des autorisations spécifiques aux baies de périphériques ou d'interconnexion et avec un de trois niveaux de privilège : administrateur, opérateur ou utilisateur. Un compte avec des privilèges d'administrateur comprenant l'autorisation de baie du module Onboard Administrator peut créer ou modifier tous les comptes utilisateur sur un boîtier. Les privilèges d'opérateur permettent d'accéder et de contrôler l'intégralité des informations relatives aux baies autorisées. Les privilèges utilisateur n'autorisent que l'accès aux informations (aucune possibilité de contrôle).

Le module Onboard Administrator impose à l'utilisateur une connexion à l'interface utilisateur Web ou CLI avec un compte et un mot de passe. Le compte peut être un compte local où le mot de passe est enregistré sur le module Onboard Administrator, ou un compte LDAP, où le module Onboard Administrator contacte le serveur LDAP défini pour vérifier les informations d'identification de l'utilisateur. L'authentification à deux facteurs permet un niveau de sécurité encore plus élevé pour la session de gestion de l'utilisateur sur le module Onboard Administrator. Vous pouvez également configurer l'authentification à deux facteurs et l'authentification LDAP, tel que décrit dans la section « Authentification TFA+LDAP » (Authentification TFA+LDAP à la page 427).

Au lieu d'imposer des connexions séparées pour accéder à plusieurs ressources (une fois à chaque boîtier et/ou une fois à chaque processeur de gestion de serveur), le module Onboard Administrator permet la connexion avec un point d'accès unique pour les boîtiers liés dans un rack. L'administrateur peut ainsi utiliser l'authentification unique pour se connecter à un module Onboard Administrator unique et utiliser l'interface utilisateur Web pour consulter et superviser les composants HP BladeSystem c-Class sur un maximum de sept boîtiers liés. (L'authentification unique exige que tous les administrateurs du module Onboard actif du boîtier disposent du même mot de passe.) Par exemple, un administrateur peut propager automatiquement les commandes de gestion, telles que la modification du mode d'alimentation du boîtier, dans tous les boîtiers liés. Un compte valide doit être présent sur chaque boîtier lié pour obtenir un accès. Pour plus d'informations, reportez-vous à la section « Connexion à l'interface graphique utilisateur Onboard Administrator » (Connexion à l'interface du module Onboard Administrator à la page 9).

Sécurité de la connexion

Le module Onboard Administrator propose plusieurs fonctions pour assurer la sécurité de la connexion. Aucune pénalité n'est imposée après un échec de tentative de connexion initiale. Avec tous les échecs de tentatives ultérieures, le module Onboard Administrator impose un délai de 10 à 30 secondes. Une page d'information s'affiche pendant chaque délai d'attente. Cette action se poursuit jusqu'à l'ouverture d'une session valide. Cette fonction aide à se défendre contre les éventuelles attaques par dictionnaire.

Le module Onboard Administrator enregistre une entrée de journal détaillée de tous les échecs de tentative de connexion.

Première exécution du module Onboard Administrator

L'installation d'un boîtier c-Class à l'aide du module Onboard Administrator est simplifiée grâce à l'utilisation de l'assistant de première installation du module Insight Display, suivie par l'utilisation de l'assistant de première installation de l'interface du module Onboard Administrator ou de l'interface CLI du module Onboard Administrator pour finaliser la réinitialisation des paramètres du boîtier.

Lors d'un fonctionnement en mode FIPS, configurez le mode FIPS avant d'effectuer toute configuration de module Onboard Administrator ou autre boîtier, y compris la configuration de l'assistant de première installation ou Virtual Connect. L'activation du mode FIPS sur un module Onboard Administrator ou une paire redondante de modules force la réinitialisation des modules Onboard Administrator sur les paramètres par défaut. Suite à la configuration du mode FIPS, effectuez les étapes de configuration de cette section. Pour plus d'informations sur le mode FIPS, consultez la section « Onglet FIPS » (Onglet FIPS à la page 139).

Les modules Onboard Administrator, les processeurs de supervision iLO des lames de serveur et de nombreux modules d'interconnexion prennent par défaut le paramètre DHCP pour leur adresse IP de supervision. Si l'utilisateur utilise le paramètre DHCP et connecte le port de supervision Onboard Administrator au serveur DHCP, les modules Onboard Administrator, tous les modules iLO et d'interconnexion qui prennent en charge et qui sont configurés pour utiliser le réseau de supervision interne du module Onboard Administrator obtiendront automatiquement des adresses DHCP du serveur DHCP de l'utilisateur.

Si vous n'avez pas de serveur DHCP pour affecter des adresses IP aux processeurs de supervision, vous devez configurer chaque adresse IP de module Onboard Administrator, puis toutes les adresses IP de supervision des modules d'interconnexion et des périphériques individuels en utilisant l'une des méthodes suivantes :

- Méthode recommandée - configurez chaque module Onboard Administrator avec une adresse IP statique à l'aide du module Insight Display. Connectez-vous ensuite à l'interface du module Onboard Administrator et utilisez l'assistant First Time Setup (Première installation) ou connectez-vous à l'interface CLI du module Onboard Administrator et configurez et activez les adresses EBIPA (Enclosure Bay IP Addresses) pour les baies de périphériques et d'interconnexion. L'activation des adresses EBIPA pour une baie permettra de remplacer ce serveur ou module d'interconnexion et le nouveau module obtiendra automatiquement l'adresse IP configurée précédemment pour cette baie.
- Vous pouvez également configurer manuellement chaque périphérique et module d'interconnexion avec une adresse IP statique. Pour les lames de serveur ProLiant, vous devez vous connecter à chaque lame de serveur à partir du port SUV (à l'aide du câble SUV fourni avec chaque boîtier) et configurer manuellement l'adresse IP iLO pendant l'opération POST en appuyant sur F8 pour accéder aux paramètres ROM de l'option iLO. Pour les modules d'interconnexion avec les processeurs de supervision pouvant utiliser le réseau de supervision Onboard Administrator, accédez à ces modules et configurez leur adresse IP à l'aide d'un port de console série externe ou la connexion série d'interface CLI du module Onboard Administrator à cette baie. Après avoir modifié manuellement l'adresse IP de module d'interconnexion, le commutateur peut nécessiter une mise hors puis sous tension pour que le nouveau paramètre soit pris en compte.

REMARQUE : Ne configurez pas l'adresse IP pour tout module Onboard Administrator dans la plage 169.254.x.x.

Les informations de connexion initiales pour se connecter à un nouveau module Onboard Administrator sont imprimées sur une étiquette sur chaque module. L'utilisateur est Administrateur et le mot de passe est unique à chaque module. Ce mot de passe doit être capturé par le programme d'installation et communiqué à l'administrateur à distance pour la première connexion à distance à l'interface du module Onboard Administrator ou à l'interface CLI du module Onboard Administrator.

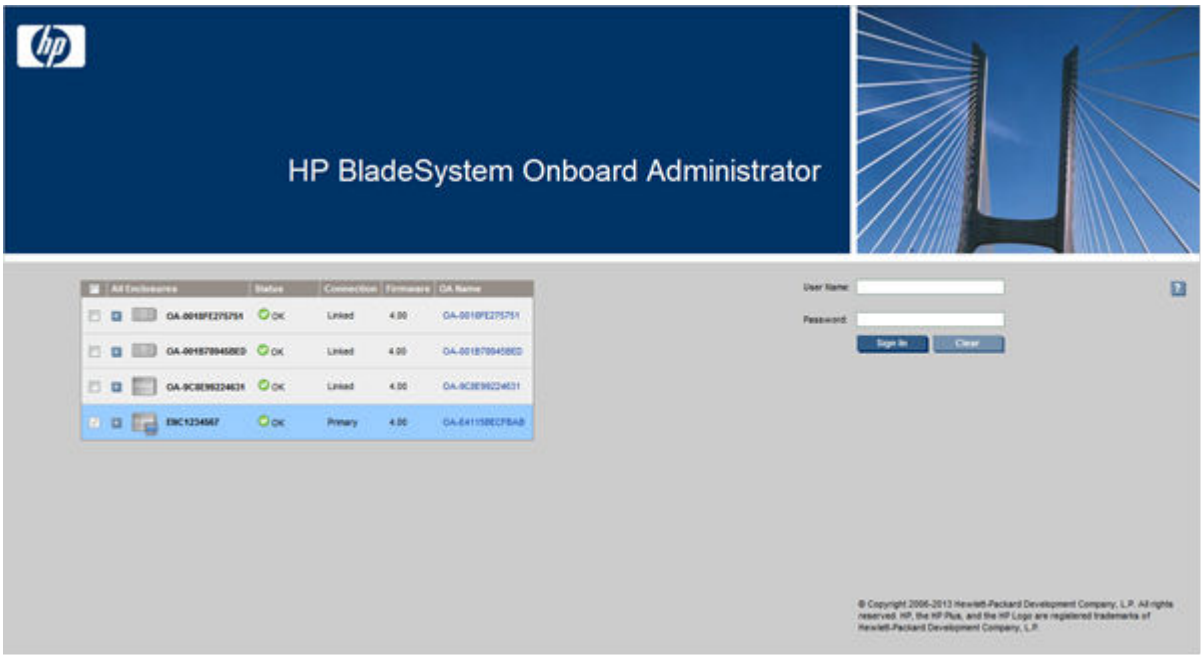
Les paramètres du boîtier peuvent être configurés manuellement ou téléchargés à partir d'un script ou d'un fichier de configuration. L'interface utilisateur Web offre un assistant First Time Setup (Première installation). L'interface CLI est accessible depuis le port série du module Onboard Administrator, le port de supervision Ethernet, le port de service, ou en utilisant le bouton Enclosure KVM - Onboard Administrator CLI (KVM de boîtier - CLI de module Onboard Administrator).

Outre la configuration manuelle, il est possible de télécharger un fichier de configuration de boîtier vers le module Onboard Administrator actif à l'aide de l'interface utilisateur graphique ou de la ligne de commande en spécifiant un emplacement HTTP, FTP ou réseau TFTP pour le fichier de configuration. Il est également possible d'utiliser l'interface utilisateur, la ligne de commande ou encore le module Insight Display pour télécharger un fichier de configuration depuis une clé USB connectée au port USB du module Onboard Administrator actif.

La méthode recommandée pour créer un fichier de configuration de boîtier consiste à utiliser l'interface utilisateur, l'interface de ligne de commande (CLI) ou le menu USB du module Insight Display pour enregistrer la configuration existante dans un fichier. Le fichier de configuration enregistré est un jeu de commandes texte CLI pour chaque élément de configuration. Le module Onboard Administrator n'enregistre pas de mots de passe de l'utilisateur lorsqu'il enregistre un fichier de configuration. L'utilisateur peut modifier le fichier de configuration et insérer les commandes de mot de passe pour chaque compte utilisateur - ou utiliser le compte local Administrateur pour mettre à jour individuellement tous les mots de passe de l'utilisateur après avoir restauré un fichier de configuration de boîtier enregistré précédemment.

Si le boîtier contient des modules Onboard Administrator redondants, le module Onboard Administrator restant met à jour le nouveau module Onboard Administrator avec tous les paramètres.

Connexion à l'interface du module Onboard Administrator



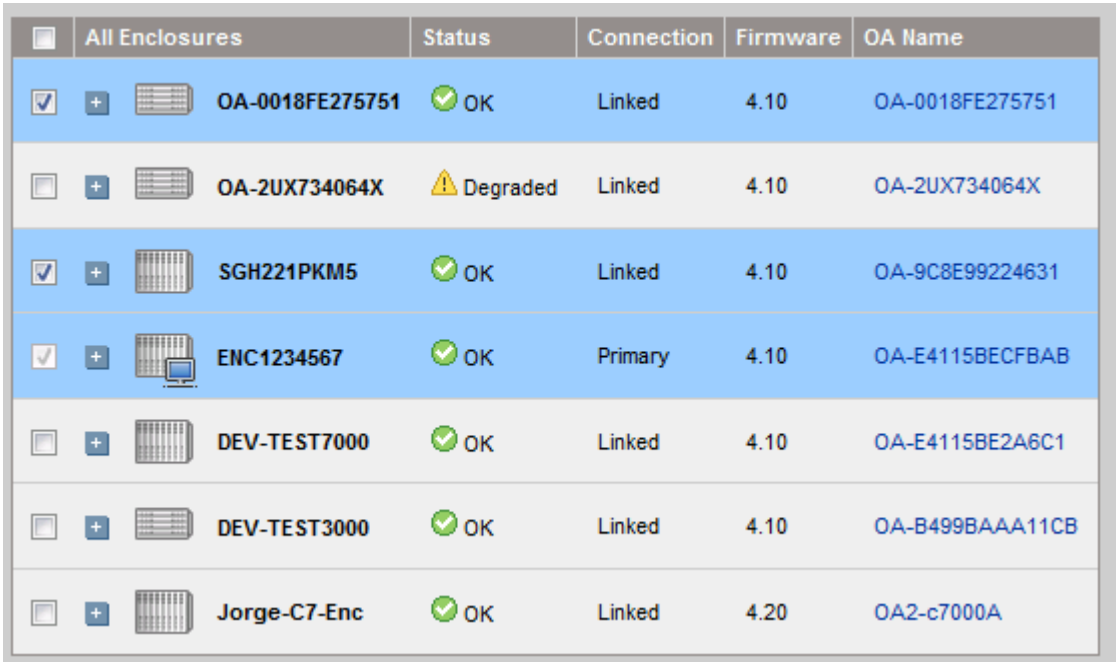
Saisissez le nom d'utilisateur et le mot de passe d'administration initial pour le module Onboard Administrator. Les informations d'identification de compte par défaut sont disponibles sur l'étiquette apposée au module Onboard Administrator.

Lors de la connexion au module Onboard Administrator, les problèmes suivants peuvent se produire :

- Vous ne saisissez pas les informations correctement. Les mots de passe font la distinction entre les majuscules et les minuscules.
- Les informations du compte que vous saisissez n'ont pas été configurées pour HP BladeSystem Onboard Administrator.
- Le nom d'utilisateur que vous saisissez a été supprimé, désactivé ou verrouillé.
- Le mot de passe de ce compte doit être modifié.
- Vous tentez de vous connecter à partir d'une adresse IP qui n'est pas correcte pour le compte spécifié.
- Vous avez perdu ou oublié le mot de passe du compte administrateur. Pour réinitialiser le mot de passe Administrateur, reportez-vous à la section « Récupération du mot de passe administrateur » (Récupération du mot de passe administrateur à la page 14).

Si les problèmes de connexion persistent, contactez votre administrateur.

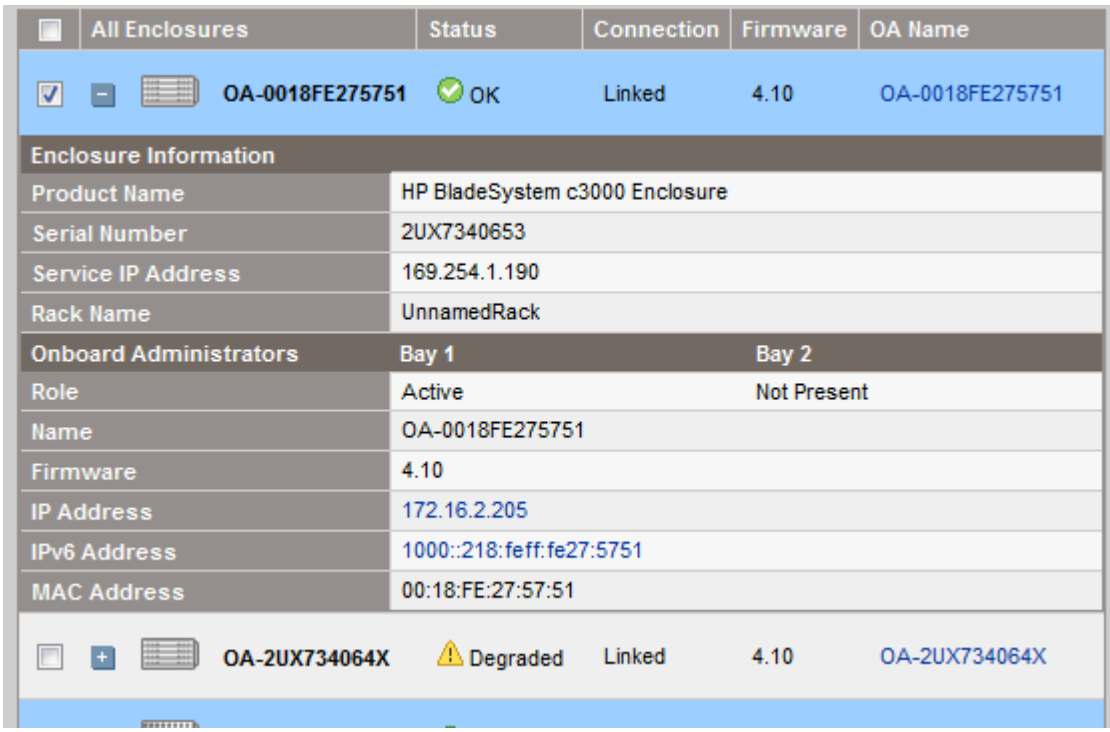
Si vous disposez des mêmes informations d'identification sur plusieurs boîtiers, vous pouvez utiliser l'authentification unique pour ouvrir une session sur plusieurs boîtiers liés. Avant de vous connecter, activez la case à côté de chacun des boîtiers reliés répertoriés dans le tableau sur la page de connexion, comme illustré dans le tableau suivant. Dans ce scénario, vous essayez de vous connecter à trois modules Onboard Administrator actifs sur les boîtiers correspondants, en utilisant le nom d'utilisateur et le mot de passe fournis. Autrement, pour vérifier et vous connecter à tous les boîtiers liés, activez la case en haut de la colonne des cases à cocher. Si la connexion réussit, chacun de ces boîtiers est affiché dans la même fenêtre d'interface utilisateur. L'ordre de positionnement de chaque boîtier est basé sur les câbles du lien du boîtier. Connectez le port de la « liaison descendante » du boîtier principal au port de la « liaison montante » du boîtier suivant. Répétez jusqu'à atteindre le boîtier inférieur. Cet ordre de l'interface graphique utilisateur est le même qui apparaît dans la commande `SHOW TOPOLOGY`.



All Enclosures	Status	Connection	Firmware	OA Name
OA-0018FE275751	OK	Linked	4.10	OA-0018FE275751
OA-2UX734064X	Degraded	Linked	4.10	OA-2UX734064X
SGH221PKM5	OK	Linked	4.10	OA-9C8E99224631
ENC1234567	OK	Primary	4.10	OA-E4115BECFBAB
DEV-TEST7000	OK	Linked	4.10	OA-E4115BE2A6C1
DEV-TEST3000	OK	Linked	4.10	OA-B499BAAA11CB
Jorge-C7-Enc	OK	Linked	4.20	OA2-c7000A

Comme illustré dans l'exemple précédent, le tableau de boîtier situé sur la page de connexion fournit également des informations sur l'état du boîtier, la connexion, la version du microprogramme, le nom OA et la position du rack. Si l'option de données étendues a été sélectionnée sur l'onglet Anonymous Data (Donnés anonymes) de la page Network Access (Accès réseau), vous pouvez voir des informations plus détaillées sur le boîtier et le module Onboard Administrator en sélectionnant le symbole sur la gauche de l'icône du boîtier. Le symbole apparaît uniquement si les données étendues sont activées sur ce boîtier. Via la page Location Discovery Services, les données étendues incluent des informations de localisation pour chaque châssis. Pour plus d'informations sur la fonction Location Discovery Services, reportez-vous à la section « Écran Rack Overview » (Écran Rack Overview à la page 102). Les données étendues sont activées par défaut. Si les données étendues sont désactivées sur un boîtier, l'état du boîtier apparaît en tant que `N/A`.

Le schéma suivant illustre les données étendues du premier boîtier répertorié dans le tableau.



Récupération flash d'urgence

Pour récupérer avec succès un module Onboard Administrator à partir d'un échec d'opération flash, vous devez disposer des éléments suivants :

- Accès local au boîtier
- Serveur DHCP accessible par le module Onboard Administrator
- Serveur TFTP accessible par le module Onboard Administrator
- Microprogramme Onboard Administrator (fichier .bin)

Pour récupérer à partir d'un échec d'opération flash, utilisez un des processus suivants :

- Si vous disposez d'un seul module Onboard Administrator dans le boîtier ou que vous souhaitez effectuer une récupération flash du module OA actif :

a. À l'aide d'un câble null-modem (9600 N, 8, 1, VT100), connectez-vous localement au module Onboard Administrator.

b. Appuyez sur le bouton de réinitialisation du module Onboard Administrator et maintenez-le enfoncé pendant 5 secondes.

c. Sur la console série, lorsque vous êtes invité à choisir une récupération flash ou à réinitialiser le mot de passe, appuyez sur **F**. Le module Onboard Administrator obtient une adresse IP via DHCP.

d. À l'invite de l'adresse IP du serveur FTP (sur lequel sont stockés les fichiers image du module Onboard Administrator), entrez l'adresse IP appropriée.

e. Vous êtes invité à spécifier le chemin d'accès à l'image du microprogramme du module Onboard Administrator. Le module Onboard Administrator télécharge l'image et clignote.

À l'issue de ce processus, le microprogramme du module Onboard Administrator est à jour et toute condition d'erreur est résolue.

- Si vous disposez de deux modules Onboard Administrator dans le boîtier et que vous souhaitez effectuer une récupération flash du module OA actif :

  a. À l'aide d'un câble null-modem (9600 N, 8, 1, VT100), connectez-vous localement au module Onboard Administrator.

  b. Appuyez sur le bouton de réinitialisation du module Onboard Administrator et maintenez-le enfoncé pendant 5 secondes.

  c. Sur la console série, lorsque vous êtes invité à choisir Flash Recovery (Récupération Flash) ou Reset Password (Réinitialiser le mot de passe), n'entrez rien. Attendez 2 minutes ou plus pour laisser le module OA en mode Standby devenir le module OA actif avant de passer à l'étape suivante.

  d. Lorsque le module OA auquel appliquer l'opération flash devient le module OA en mode Standby, appuyez une deuxième fois sur le bouton de réinitialisation sur le même module OA qu'à l'étape b et maintenez-le enfoncé.

  e. Sur la console série, lorsque vous êtes invité à choisir une récupération flash ou à réinitialiser le mot de passe, appuyez sur **F**. Le module Onboard Administrator obtient une adresse IP via DHCP.

  f. À l'invite de l'adresse IP du serveur FTP (sur lequel sont stockés les fichiers image du module Onboard Administrator), entrez l'adresse IP appropriée.

  g. Vous êtes invité à spécifier le chemin d'accès à l'image du microprogramme du module Onboard Administrator. Le module Onboard Administrator télécharge l'image et clignote.

À l'issue de ce processus, le microprogramme du module Onboard Administrator est à jour et toute condition d'erreur est résolue.

REMARQUE : Le module Onboard Administrator avec le microprogramme version 4.50 ou ultérieure ne prend pas en charge la récupération flash d'urgence vers une version 4.50 ou ultérieure du microprogramme. Si vous utilisez une version 4.50 ou ultérieure du microprogramme, effectuez une récupération flash vers une version antérieure à 4.50, puis mettez à jour votre microprogramme dans la version souhaitée (4.50 ou ultérieure).

Exécution de l'assistant d'installation

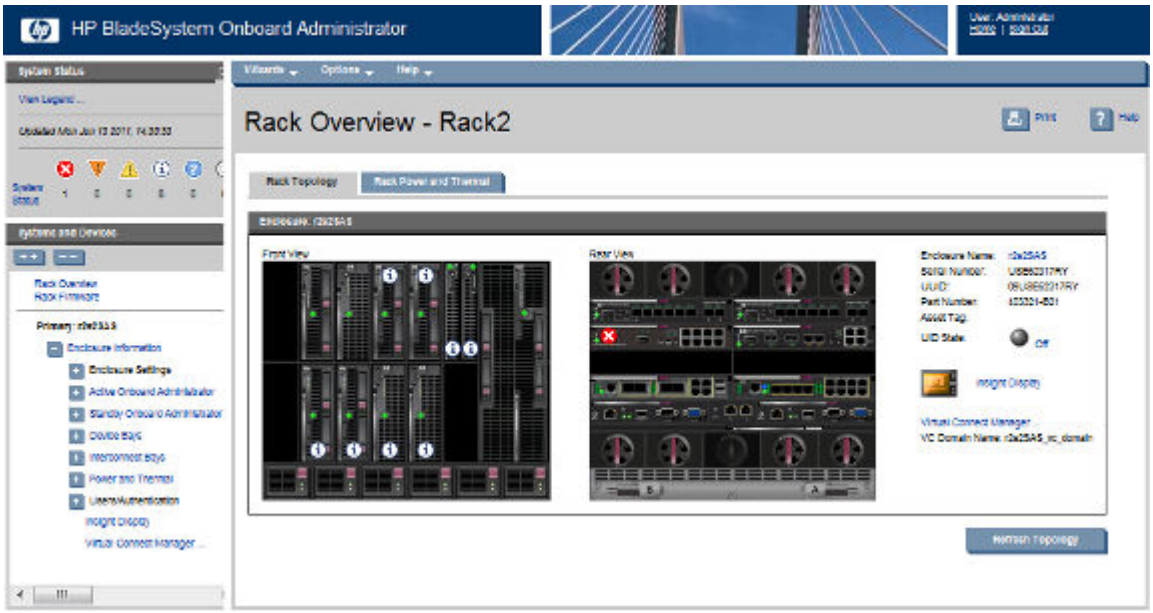
Pour exécuter l'assistant d'installation, connectez-vous à Onboard Administrator. L'assistant First Time Setup (Assistant de première installation) démarre automatiquement lors de votre première

connexion à Onboard Administrator. Cet assistant vous guide dans la configuration de toutes les fonctions du module Onboard Administrator. Vous pouvez accéder à cet assistant d'installation à tout moment après l'installation initiale en cliquant sur le lien **Wizards** (Assistants) en haut à gauche de l'écran central.

Pour obtenir des informations détaillées, reportez-vous à la section « Assistant First Time Setup » (Assistant de première installation) (Assistant First Time Setup à la page 54).

Utilisation de l'aide en ligne

Pour accéder à l'aide en ligne, cliquez sur le point d'interrogation blanc sur fond bleu ou **Help** (Aide) en haut à droite de l'écran, sous la barre d'en-tête. L'aide en ligne affiche les informations liées à la section du module Onboard Administrator dans lequel vous naviguez.



Modification de la configuration du boîtier et des périphériques

Une fois que vous avez exécuté l'assistant First Time Setup, vous pouvez revenir à tout moment dans l'interface du module Onboard Administrator pour modifier la configuration. Pour plus d'informations sur la modification de la configuration du boîtier et des périphériques, de la configuration utilisateur, ainsi que des paramètres de serveur LDAP et des groupes LDAP, consultez la section « Configuration des boîtiers HP BladeSystem c7000 et des périphériques de boîtier » (Configuration des boîtiers HP BladeSystem et des périphériques de boîtier à la page 112).

Pour obtenir plus d'informations sur les paramètres d'alimentation de boîtier, reportez-vous à la section « Gestion de l'alimentation de boîtier » (Gestion de l'alimentation de boîtier à la page 300).

Récupération du mot de passe administrateur

Si le mot de passe administrateur a été perdu, vous pouvez réinitialiser le mot de passe administrateur sur la valeur usine par défaut qui a été fournie sur l'étiquette avec le module Onboard Administrator. Le module Onboard Administrator redéfinit un mot de passe perdu en mode Lost Password/Flash Disaster Recovery (LP/FDR) (Perte du mot de passe/Récupération flash d'urgence). Pour réinitialiser le mot de passe administrateur à la valeur usine par défaut :

1. Connectez un ordinateur au port série du module Onboard Administrator actif à l'aide d'un câble null-modem.
2. À l'aide d'un câble null-modem (9600 N, 8, 1, VT100), connectez-vous localement au module Onboard Administrator.
3. Ouvrez un utilitaire de fenêtre du terminal approprié (Windows ou Linux) et connectez-vous au module Onboard Administrator actif.
4. Appuyez sur le bouton de réinitialisation du module Onboard Administrator et maintenez-le enfoncé pendant 5 secondes.
5. Pour démarrer le système en mode Lost Password (Mot de passe perdu), appuyez sur **L.** Le mot de passe apparaît au redémarrage du système.

Sinon, pour réinitialiser un mot de passe sur le module Onboard Administrator, sélectionnez l'option Menu USB de l'écran Insight Display (panneau LCD). Cette option restaure un script de configuration à l'aide des commandes de l'interface de ligne de commande stockées sur une clé USB.

REMARQUE : Si les boutons du menu USB de l'écran Insight Display sont verrouillés, la méthode du port série doit être utilisée. Si le panneau LCD est verrouillé, un important symbole de « verrou » apparaît sur l'écran.

Dans cet exemple, le mot de passe administrateur OA est défini sur `Mot_passe123`.

1. Créez un fichier texte appelé `reset_password.cfg` avec la commande d'une ligne : `SET USER PASSWORD` "Administrateur" "Mot_passe123".
2. Insérez le lecteur flash avec le fichier `reset_password.cfg` dans le port USB du module Onboard Administrator actif. Le voyant sur le module Onboard Administrator indique quel module OA est actif.
3. À l'aide de l'écran Insight Display du module Onboard Administrator, naviguez vers le menu principal, sélectionnez le menu USB Key (Clé USB), puis cliquez sur **OK.**
4. Si la protection PIN de l'écran Insight Display est activée, vous êtes invité à saisir le code PIN. Sélectionnez **Accept** (Accepter) puis cliquez sur **OK.**

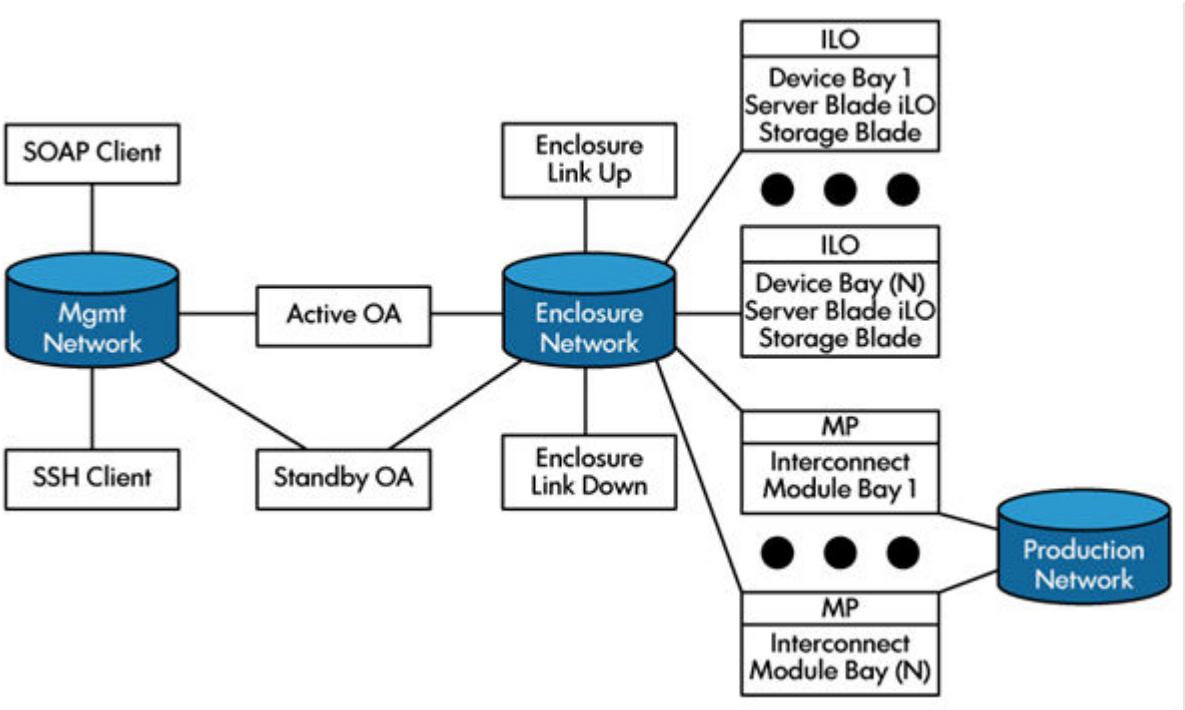
5. Sélectionnez **Restore Configuration** (Restaurer la configuration), puis cliquez sur **OK**. Le lecteur flash USB dans le module Onboard Administrator est analysé et les fichiers .cfg disponibles sont répertoriés.
6. Sélectionnez le fichier `reset_password.cfg`, puis cliquez sur **OK**.
7. L'écran de confirmation de l'opération apparaît, cliquez sur **OK**.
8. Connectez-vous au module Onboard Administrator avec l'ID et le mot de passe utilisateur spécifiés à l'étape 1.

Considérations de sécurité

Cette section décrit les recommandations d'architecture et de meilleure pratique de sécurité à prendre en considération lors de la configuration du module Onboard Administrator et compare les paramètres par défaut avec les versions précédentes.

Présentation de l'architecture de réseau BladeSystem

L'ensemble des baies de périphérique, modules d'interconnexion et modules Onboard Administrator sont connectés à un réseau interne de boîtiers qui est géré par le module Onboard Administrator actif. Le trafic réseau provenant d'applications d'entreprise exécutées sur des lames de serveur est acheminé à travers des modules de commutation d'interconnexion et sur le réseau de production.



Bien qu'il soit possible pour des réseaux de gestion et de production d'être connectés, le réseau de gestion doit être isolé du trafic de production et de l'intranet. Du point de vue de la sécurité, ceci réduit l'accès et la capacité d'attaquer les interfaces de gestion. Par souci d'efficacité, des réseaux distincts maintiennent le trafic de production hors du réseau de gestion.

Pratiques d'excellence de sécurité recommandées

En plus des meilleures pratiques, prenez note de ces considérations supplémentaires.

Considérations de présence physique

L'accès physique à un système implique souvent des privilèges d'administrateur. Le module Onboard Administrator ne fait pas exception. Pour plus d'informations sur la façon de configurer l'administrateur Onboard Administrator, consultez la section « Configuration des boîtiers HP BladeSystem c7000 et des périphériques de boîtier » (Configuration des boîtiers HP BladeSystem et des périphériques de boîtier à la page 112).

- Vérification du câblage physique

  Le boîtier BladeSystem peut avoir plusieurs câbles reliés au boîtier. Les câbles raccordés aux modules de commutation d'interconnexion sont en général pour le trafic du réseau de production. Tous les autres câbles et ports sont généralement destinés au trafic du réseau de gestion du boîtier et doivent être soigneusement inspectés.

  - Assurez-vous que les ports de liaison de boîtier sont uniquement reliés à des ports de liaison de boîtier sur d'autres boîtiers.
  - Inspectez les ports série Onboard Administrator pour détecter les connexions non autorisées.
  - Inspectez les ports USB Onboard Administrator pour détecter les connexions non autorisées.

- Fixation du panneau LCD Insight Display

  Le panneau LCD de l'écran Insight Display permet la configuration et la surveillance des paramètres clés du module Onboard Administrator : configuration de l'adresse de réseau et mise sous/hors tension des baies de lame du serveur pour nommer quelques fonctions critiques de BladeSystem. HP recommande de fixer le panneau LCD Insight Display avec un code PIN, en particulier dans un centre de données multi-locataire. Par ailleurs, certaines normes réglementaires ou de l'industrie, telles que PCI, peuvent exiger que toutes les interfaces soient sécurisées avec un code PIN/mot de passe, quelles que soient les exigences d'accès physique.

  Les boutons du panneau LCD Insight Display sont verrouillés par défaut en mode FIPS ON/DEBUG. Pour plus d'informations, consultez la section « Onglet FIPS » (Onglet FIPS à la page 139).

Définition des paramètres usine par défaut avant le redéploiement du matériel

La nature même du matériel redondant est de s'assurer que tous les paramètres sont présents de sorte que si une panne se produit sur le module Onboard Administrator actif, le module Onboard Administrator en Standby peut prendre en charge le rôle actif. Cela signifie que les informations de compte utilisateur local sont dupliquées sur le module Onboard Administrator en Standby. Si le mode IP du boîtier est configuré, la clé privée utilisée pour les communications SSL est également stockée sur le module Onboard Administrator en Standby. (Le mode IP du boîtier n'est pas configuré par défaut.) Selon les exigences de sécurité pour le centre de données, les paramètres de sécurité critiques doivent être effacés du matériel avant la désaffectation ou le réapprovisionnement d'un boîtier ou des composants dans le boîtier, tels que le module Onboard Administrator, le module VC et iLO pour HP BladeSystem.

Pour s'assurer que tous les paramètres de sécurité critiques sont effacés, utilisez la commande SET FACTORY. De plus, le mot de passe Administrateur peut être défini sur la valeur usine « toe-tag » en modifiant manuellement le mot de passe ou en connectant un câble série et en invoquant la procédure de récupération de mot de passe perdu. Pour obtenir des instructions, consultez la section « Récupération du mot de passe administrateur » (Récupération du mot de passe administrateur à la page 14).

Isolation du réseau de gestion

Peu importe comment un périphérique peut sembler être sécurisé, il y aura toujours une sorte de nouvelle attaque ou vulnérabilité. En tant que mesure préventive et pour suivre les meilleures pratiques de l'industrie, HP recommande fortement que le réseau de gestion soit distinct du réseau de production. De plus, ne placez pas le réseau de gestion sur la zone DMZ du pare-feu ou l'Internet ouvert sans nécessiter d'authentification d'accès supplémentaire, telle que l'utilisation d'un VPN/ tunnel.

Ports réseau

Pour plus d'informations sur les ports, consultez la section « Exigences d'accès » (Exigences d'accès à la page 3).

Pour plus d'informations sur la gestion de logiciels HP à travers un pare-feu, consultez le livre blanc *Managing HP Servers Through Firewalls with Insight Management* (Gestion de serveurs HP à travers des pare-feu avec Insight Management). Ce document peut être téléchargé à partir de la bibliothèque d'informations de HP Insight Management (http://www.hp.com/go/docs).

Fonctionnalités de sécurité cryptographique et valeurs par défaut

À compter de la version 3.71, Onboard Administrator met à niveau de manière significative les capacités cryptographiques du module Onboard Administrator par l'ajout d'un nouveau mode de fonctionnement FIPS. Le mode FIPS applique un certain nombre d'exigences qui diffèrent sensiblement des paramètres non FIPS et des versions antérieures. Les améliorations de la sécurité suppriment les algorithmes faibles et suivent généralement la norme FIPS 140-2. Pour plus d'informations, reportez-vous au tableau suivant. Une liste de chiffrements SSH pris en charge, des algorithmes d'échange de clés SSH, et des algorithmes de code d'authentification de message SSH sont indiqués sous le tableau.

L'administrateur OA peut modifier les paramètres du mode FIPS et activer ou désactiver des chiffrements et protocoles cryptographiques via l'onglet **Enclosure Settings>Network Access>FIPS** (Onglet FIPS à la page 139).

REMARQUE : Lorsque vous exécutez une version du microprogramme Onboard Administrator antérieure à la version 3.71 avec le mode de cryptage robuste activé, si vous mettez à jour le microprogramme vers une version 3.71 ou ultérieure et antérieure à 4.40, une entrée peut être enregistrée dans le journal système Onboard Administrator, indiquant que le module Onboard Administrator fonctionne en mode FIPS. Cette entrée du journal système (`FIPS: OA is operating in FIPS Mode On`) est incorrecte et peut être ignorée.

Paramètres du mode FIPS

	OA 3.71 FIPS Mode OFF	OA 3.71 FIPS Mode ON	OA 4.01-OA 4.02 FIPS Mode OFF	OA 4.01-OA 4.02 FIPS Mode ON	OA 4.11-OA 4.22 FIPS Mode OFF	OA 4.11-OA 4.22 FIPS Mode ON	OA 4.30-OA 4.50 FIPS Mode OFF	OA 4.30-OA 4.50 FIPS Mode ON
Éléments de sécurité générale								
Mise à zéro de CSP	NON	OUI	NON	OUI	NON	OUI	NON	OUI
KATs (Known Answer Tests - Tests à	NON	OUI	NON	OUI	NON	OUI	NON	OUI

	OA 3.71 FIPS Mode OFF	OA 3.71 FIPS Mode ON	OA 4.01-OA 4.02 FIPS Mode OFF	OA 4.01-OA 4.02 FIPS Mode ON	OA 4.11-OA 4.22 FIPS Mode OFF	OA 4.11-OA 4.22 FIPS Mode ON	OA 4.30-OA 4.50 FIPS Mode OFF	OA 4.30-OA 4.50 FIPS Mode ON
réponse connue)								
Tests de mise sous tension	NON	OUI	NON	OUI	OUI	OUI	OUI	OUI
Test PRNG continu	NON	OUI	NON	OUI	OUI	OUI	OUI	OUI
Longueur minimum du mot de passe	3	8	3	8	3	8	3	8
Exiger complexité du mot de passe (majuscules, minuscules, symboles)	NON	OUI	NON	OUI	NON	OUI	NON	OUI
PRNG compatible FIPS[1]	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI
Service Telnet désactivé	OUI[2]	OUI	NON[2]	OUI	OUI[2]	OUI	OUI[2]	OUI[2]
Mode IP de boîtier désactivé	NON	OUI	NON	OUI	NON	OUI	NON	OUI
Prise en charge de vidage désactivée	NON	OUI	NON	OUI	NON	OUI	NON	OUI
Services SNMPv1 et SNMPv2 désactivés	NON	OUI	NON	OUI	NON	OUI	NON	OUI
Contrôle d'intégrité de partition	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI
Exige code PIN de panneau LCD Insight Display	NON	OUI	NON	OUI	NON	OUI	NON	OUI
Chiffrement SSL								

	OA 3.71 FIPS Mode OFF	OA 3.71 FIPS Mode ON	OA 4.01-OA 4.02 FIPS Mode OFF	OA 4.01-OA 4.02 FIPS Mode ON	OA 4.11-OA 4.22 FIPS Mode OFF	OA 4.11-OA 4.22 FIPS Mode ON	OA 4.30-OA 4.50 FIPS Mode OFF	OA 4.30-OA 4.50 FIPS Mode ON
Taille de clé SSL par défaut	2048 bits	2048 bits	2048 bits	2048 bits	2048 bits	2048 bits	2048 bits	2048 bits
Algorithme de signature de hachage de certificat auto-signé par défaut	SHA256	SHA256	SHA256	SHA256	SHA256	SHA256	SHA256	SHA256
Algorithmes de signature de hachage SSL configurable sur certificat auto-signé	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI
Protocoles SSL/TLS	SSLv3 TLSv1	TLSv1	SSLv3 TLSv1	TLSv1	TLSv1 TLSv1.1 TLSv1.2	TLSv1 TLSv1.1 TLSv1.2	TLSv1 TLSv1.1 TLSv1.2	TLSv1 TLSv1.1 TLSv1.2
Rejet des certificats avec algorithmes de signature de hachage non FIPS[3]	NON	OUI	NON	OUI	NON	OUI	NON	OUI
Algorithmes de hachage de signature de certificat autorisés	md5,sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	md5, sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512
DES	NON	NON	NON	NON	NON	NON	NON	NON
CAST5	NON	NON	NON	NON	NON	NON	NON	NON
Blowfish	NON	NON	NON	NON	NON	NON	NON	NON
ARC4	NON	NON	NON	NON	NON	NON	NON	NON
3DES	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI
AES 128-SHA	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI
DHE-RSA-AES256-SHA	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI - version 4.30

	OA 3.71 FIPS Mode OFF	OA 3.71 FIPS Mode ON	OA 4.01-OA 4.02 FIPS Mode OFF	OA 4.01-OA 4.02 FIPS Mode ON	OA 4.11-OA 4.22 FIPS Mode OFF	OA 4.11-OA 4.22 FIPS Mode ON	OA 4.30-OA 4.50 FIPS Mode OFF	OA 4.30-OA 4.50 FIPS Mode ON
								NON - version 4.40 et ultérieure
AES256-SHA	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI
DHE-RSA-AES128-SHA	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI - version 4.30 NON - version 4.40 et ultérieure
EDH-RSA-DES-CBC3-SHA	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI
DES-CBC3-SHA	OUI	OUI	OUI	OUI	OUI	OUI	NON	NON
AES128-GCM-SHA256	NON	NON	NON	NON	NON	NON	OUI	OUI
AES256-GCM-SHA384	NON	NON	NON	NON	NON	NON	OUI	OUI
AES128-SHA256	NON	NON	NON	NON	NON	NON	OUI	OUI
AES256-SHA256	NON	NON	NON	NON	NON	NON	OUI	OUI
Interface SSH								
Type et taille de la clé SSH par défaut	DSA 2048	DSA 1024	DSA 2048	DSA 1024	RSA 2048	RSA 2048	RSA 2048	RSA 2048
HMAC-MD5	NON	NON	NON	NON	NON	NON	NON	NON
HMAC-SHA1-96	NON	NON	NON	NON	NON	NON	NON	NON
HMAC-SHA1	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI
HMAC-SHA256	NON	NON	NON	NON	OUI	OUI	OUI	OUI
HMAC-SHA512	NON	NON	NON	NON	OUI	OUI	OUI	OUI

	OA 3.71 FIPS Mode OFF	OA 3.71 FIPS Mode ON	OA 4.01-OA 4.02 FIPS Mode OFF	OA 4.01-OA 4.02 FIPS Mode ON	OA 4.11-OA 4.22 FIPS Mode OFF	OA 4.11-OA 4.22 FIPS Mode ON	OA 4.30-OA 4.50 FIPS Mode OFF	OA 4.30-OA 4.50 FIPS Mode ON
KVM Insight Display								
Chiffrement RC4	OUI	NON	OUI	NON	OUI	NON	OUI	NON
Prise en charge AES pour KVM LCD	OUI	OUI	OUI	NON	OUI	OUI	OUI	OUI

[1] X9.31 a été utilisé dans OA 3.71 et OA 4.01-4.02. À partir de OA 4.11, AES CTR DRBG compatible SP800-90A est utilisé.
[2] Telnet est désactivé par défaut dans Onboard Administrator version 3.70 et ultérieure. Si en mode FIPS, Telnet ne peut pas être activé.
[3] Algorithme de hachage de certificat par défaut modifié de SHA1 en SHA256 dans Onboard Administrator 3.70. Vous pouvez sélectionner différentes tailles de clés et différents algorithmes de hachage avec la commande `GENERATE KEY` (GÉNÉRER LES CLÉS).

Onboard Administrator 4.40 modifie le nom d'affichage des chiffrements TLS pris en charge, et introduit un ordre strict à suivre par les chiffrements TLS activés. La liste des chiffrements TLS pris en charge et leur ordre est fourni dans le tableau suivant.

Suites de chiffrements TLS	OA 4.40 - 4.50 mode FIPS désactivé	OA 4.40 - 4.50 mode FIPS activé
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	OUI	OUI
TLS_RSA_WITH_AES_128_CBC_SHA	OUI	OUI
TLS_RSA_WITH_AES_256_CBC_SHA	OUI	OUI
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	OUI	NON
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	OUI	NON
TLS_RSA_WITH_AES_128_GCM_SHA256	OUI	OUI
TLS_RSA_WITH_AES_256_GCM_SHA384	OUI	OUI
TLS_RSA_WITH_AES_128_CBC_SHA256	OUI	OUI
TLS_RSA_WITH_AES_256_CBC_SHA256	OUI	OUI

Chiffres SSH

Les jeux de chiffrement SSH pris en charge sont identiques pour le mode FIPS activé et le mode FIPS désactivé, et pour Onboard Administrator versions 3.71, 4.01 - 4.02, 4.11 - 4.22 et 4.30 - 4.50 :

- `aes128-ctr`
- `aes192-ctr`
- `aes256-ctr`
- `aes128-cbc`

- `3des-cbc`
- `aes192-cbc`
- `aes256-cbc`
- `rijndael-cbc@lysator.liu.se`

Algorithmes d'échange de clé SSH

- OA 4.30 - 4.50

  `ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1`

- OA 4.11 - 4.22

  `diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1`

- OA 4.01 - 4.02

  `diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1`

- OA 3.71

  `diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1`

  - OA 4.01 et les versions ultérieures incluent une option pour activer/désactiver `diffie-hellman-group1-sha1`.
  - La valeur par défaut de OA 4.01 et 4.02 pour `diffie-hellman-group1-sha1` est désactivée.
  - La valeur par défaut de OA 4.11 - 4.22 et 4.30 - 4.50 pour `diffie-hellman-group1-sha1` est activée si le mode FIPS est désactivé ; elle est désactivée si le mode FIPS est activé.

Algorithmes de code d'authentification de message SSH

Le code d'authentification de message SSH pris en charge est identique pour le mode FIPS activé et le mode FIPS désactivé. Onboard Administrator 3.70 et versions ultérieures ne prend plus en charge HMAC-MD5 et HMAC-SHA-96 pour l'authentification des messages SSH2.

- OA 4.11 - 4.22 et 4.30 - 4.50

  `hmac-sha2-256`

  `hmac-sha2-512`

  `hmac-sha1`

- OA 4.01 - 4.02

  `hmac-sha1`

- OA 3.71

  `hmac-sha1`

2 Installation matérielle des boîtiers HP BladeSystem c3000/c7000

Installation de modules Onboard Administrator

Les boîtiers HP BladeSystem c3000 et HP BladeSystem c7000 sont livrés avec un module Onboard Administrator HP BladeSystem installé et peuvent prendre en charge jusqu'à deux modules Onboard Administrator. Installez les modules Onboard Administrator en fonction du nombre total commandé :

- Un module Onboard Administrator : baie 1
- Deux modules Onboard Administrator : baies 1 et 2

Installez une découpe de module Onboard Administrator dans une baie de module Onboard Administrator inutilisé.

REMARQUE : Lorsque deux modules Onboard Administrator sont installés, le module installé dans la baie 1 est actif et celui installé dans la baie 2 est redondant.

Les instructions d'installation d'un module Onboard Administrator sont disponibles dans les documents suivants, accessibles à partir de la Bibliothèque d'informations de HP BladeSystem (http://www.hp.com/support/BladeSystem/docs) :

- *Manuel d'installation et de configuration du boîtier HP BladeSystem c3000*
- *Manuel d'installation et de configuration du boîtier HP BladeSystem c7000*

Câblage du module Onboard Administrator

Les instructions relatives au câblage d'un module OA sont disponibles dans les documents suivants, accessibles à partir de la bibliothèque d'informations de HP BladeSystem (http://www.hp.com/support/BladeSystem/docs) :

- Manuel d'installation et de configuration du boîtier HP BladeSystem c3000
- Manuel d'installation et de configuration du boîtier HP BladeSystem c7000

Si le port Ethernet de gestion du module OA est connecté à un réseau LAN de gestion qui se connecte également aux ports du serveur, assurez-vous que les applications du serveur ne surchargent pas le port de gestion OA avec des paquets de diffusion. Le module OA est le canal de gestion pour tous les périphériques internes, tels que les modules iLO et les interfaces de gestion Virtual Connect ; il doit inspecter tous les paquets en provenance du réseau. Le port de gestion OA transfère tous les paquets de diffusion à partir du réseau de gestion vers tous les périphériques à l'intérieur du boîtier. Lorsque le module OA détecte un taux élevé de paquets, il enregistre les messages de saturation de paquets de réseau dans le journal système du module OA actif. Si les connexions du serveur sont de 1 Go et que la connexion OA est de 100 Mo, les paquets de diffusion du serveur peuvent facilement saturer le port du commutateur réseau auquel le module OA est connecté. Si la saturation de paquets réseau persiste et que le module OA est saturé, les performances de ce dernier sont affectées, ce qui peut entraîner son redémarrage. Le redémarrage de l'OA n'entraîne pas d'indisponibilité du trafic client, mais peut provoquer des désagréments inutiles, en particulier dans les configurations Virtual Connect.

Si le module OA est connecté à un réseau via un serveur DHCP, ce module et chaque système iLO (un pour chaque lame de serveur) consomment un bail DHCP lorsque vous mettez le boîtier sous tension.

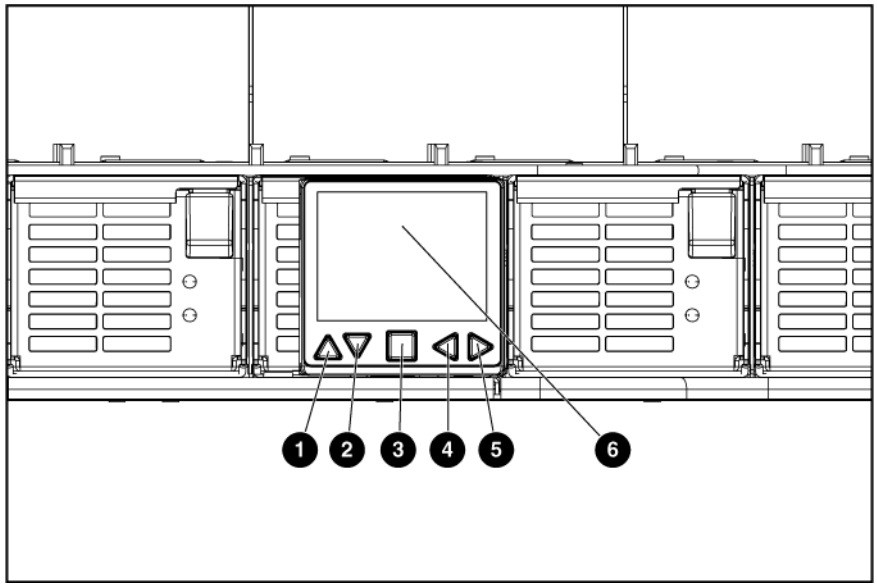
Ports Onboard Administrator

Type de port	Description	Consignes d'utilisation
OA/ILO	Connecteur RJ45 Ethernet 1000BaseT	• Fournit un accès Ethernet au module OA et à la carte iLO sur chaque lame. • Prend en charge les modules d'interconnexion avec processeurs de supervision configurés pour utiliser le réseau de supervision du boîtier. • Négociation automatique 1000/100/10 ou peut être configuré pour forcer une communication duplex intégral 100Mb ou 10Mb.
USB	Connecteur USB 2.0 de type A	Pour la connexion de périphériques USB tels que lecteurs de DVD, unités de clé USB, ou un clavier ou souris pour utilisation de boîtier KVM. La taille maximale de fichier prise en charge pour les clés USB formatées avec FAT32 est de 4 Go. Pour les images SPP supérieures à 4 Go, utilisez une clé USB de format ext2.
Connecteur série	Connecteur DB-9 RS232 série avec branchement standard pour PC.	Fournit un accès direct au module OA, à l'aide d'un câble série null-modem. Fournit un canal de communication bidirectionnelle. • Utile lorsque le module OA n'est pas accessible sur le réseau. • Permet de connecter un ordinateur à l'interface de ligne de commande (CLI) du module OA. Par exemple, le canal de communication bidirectionnelle permet aux utilisateurs d'exécuter des commandes de diagnostic ou d'afficher des informations sur l'état du boîtier. • Permet d'accéder au module OA sans besoin d'informations d'identification ni de connaître une adresse IP. Si vous avez oublié vos informations d'identification d'administrateur OA, vous pouvez vous connecter au module OA via le port série et réinitialiser le mot de passe (voir la section « Récupération du mot de passe administrateur » (Récupération du mot de passe administrateur à la page 14)).

Type de port	Description	Consignes d'utilisation
Connecteur VGA	Connecteur DB-15 VGA avec branchement standard pour PC. Les ports VGA du boîtier c3000 se trouvent sur un module distinct (le module KVM) à l'arrière du boîtier.	Similaire au port série, mais permet en outre d'accéder au module KVM du rack et au système iLO de lames de serveur. Toutefois, cela fournit uniquement un affichage ; il n'est pas possible d'exécuter des diagnostics de module OA via la connexion KVM. Pour accéder au menu KVM du boîtier, connectez un moniteur KVM de rack. Pour accéder à l'interface CLI du module OA, connectez un moniteur VGA.
Port d'interruption de liaison du boîtier	Permet de se connecter au port d'établissement de liaison situé sur le boîtier du dessous au moyen d'un cordon de raccordement CAT5.	Utilisé pour la connexion de différents boîtiers et pour la création d'un cluster de boîtiers. En liant des boîtiers, seule l'adresse IP du boîtier de base doit être connue pour accéder au groupe de boîtiers.
Port d'établissement de liaison du boîtier et port de service	Se connecte au port d'interruption de liaison situé sur le boîtier du dessus au moyen d'un cordon de raccordement CAT5.	Même utilisation que le port d'interruption de liaison du boîtier. Sur un boîtier autonome ou sur le boîtier supérieur d'une série de boîtiers liés, le port d'établissement de liaison du boîtier supérieur fonctionne comme un port de service.

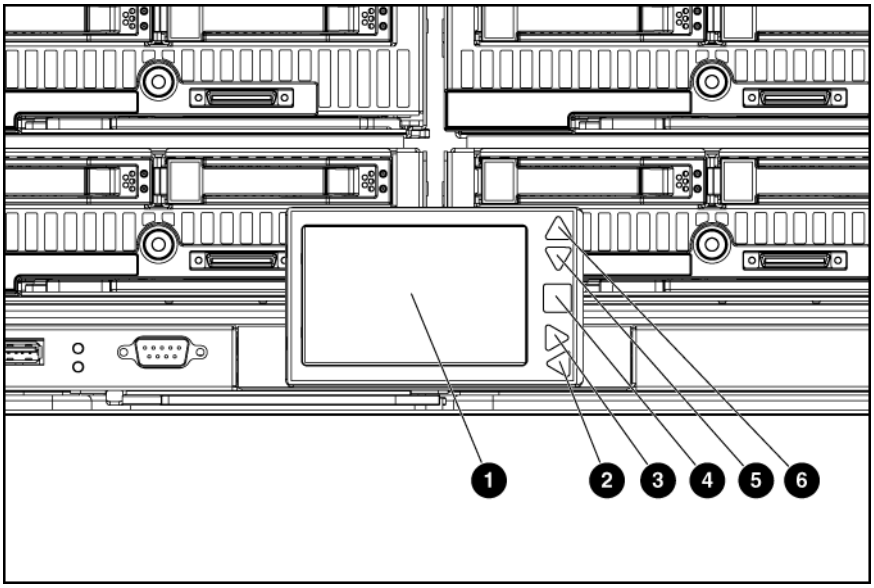
3 HP BladeSystem Insight Display

Composants de l'écran Insight Display 2 pouces du modèle HP BladeSystem c7000



Élément	Description	Fonction
1	Flèche haut (icône)	Permet de sélectionner l'option de menu immédiatement au-dessus de la sélection actuelle
2	Flèche bas (icône)	Permet de sélectionner l'option de menu immédiatement en dessous de la sélection actuelle
3	Bouton OK	Accepte la sélection en surbrillance et permet d'accéder au menu sélectionné
4	Flèche gauche (icône)	Permet de sélectionner l'option de menu ou de la barre de navigation immédiatement à gauche de la sélection actuelle
5	Flèche droite (icône)	Permet de sélectionner l'option de menu ou de la barre de navigation immédiatement à droite de la sélection actuelle
6	Écran Insight Display	Affiche les messages d'erreur du menu principal et les instructions

Composants de l'écran Insight Display 3 pouces des modèles HP BladeSystem c3000 et c7000



Élément	Description	Fonction
1	Écran Insight Display	Affiche les messages d'erreur du menu principal et les instructions
2	Flèche gauche (icône)	Permet de sélectionner l'option de menu ou de la barre de navigation immédiatement à gauche de la sélection actuelle
3	Flèche droite (icône)	Permet de sélectionner l'option de menu ou de la barre de navigation immédiatement à droite de la sélection actuelle
4	Bouton OK	Accepte la sélection en surbrillance et permet d'accéder au menu sélectionné
5	Flèche bas (icône)	Permet de sélectionner l'option de menu immédiatement en dessous de la sélection actuelle
6	Flèche haut (icône)	Permet de sélectionner l'option de menu immédiatement au-dessus de la sélection actuelle

Présentation du module Insight Display

L'écran Insight Display permet au technicien du rack d'effectuer la configuration initiale du boîtier. Il fournit également des informations sur l'intégrité et le fonctionnement du boîtier. La couleur du module Insight Display varie selon la condition de l'intégrité du boîtier :

- Bleu : le module Insight Display s'allume en bleu lorsque l'identification d'unité du boîtier est active. L'UID du boîtier est automatiquement activée lors de la première mise sous tension du

boîtier et vous pouvez l'activer en sélectionnant Turn Enclosure UID On (Activer l'UID du boîtier) dans le menu principal ou en appuyant sur le bouton UID de l'interposeur de gestion.

Une fois l'UID du boîtier activée, l'écran Insight Display clignote au bout de deux minutes d'inactivité. Pour arrêter le clignotement et réactiver l'écran, cliquez sur n'importe quel bouton de l'écran Insight Display.

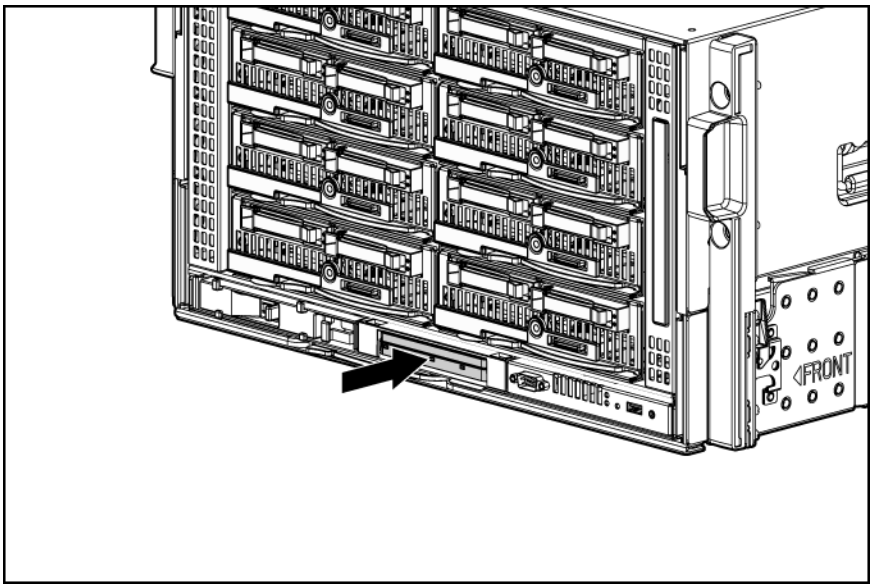
- Vert : l'écran Insight Display est vert en l'absence de toute erreur ou de condition d'alerte et lorsque le boîtier fonctionne normalement. L'écran s'éteint au bout de deux minutes d'inactivité. La pression d'un bouton sur le module Insight Display réactive l'écran.
- Orange : le module Insight Display s'allume en orange lorsque le module Onboard Administrator détecte une condition d'erreur ou d'alerte. Les détails de la condition s'affichent à l'écran.

  Après deux minutes d'inactivité, l'écran de couleur orange clignote pour indiquer la présence d'une erreur ou une condition d'alerte. Si l'UID du boîtier est active et qu'une erreur ou une condition d'alerte est détectée, l'écran devient bleu, car l'UID du boîtier est prioritaire par rapport à l'alerte. La pression d'un bouton sur le module Insight Display réactive l'écran.
- Noir (hors tension) : l'écran Insight Display dispose d'une période d'inactivité de deux minutes. Si aucune action n'est exécutée ou qu'il n'existe aucune condition d'alerte, l'écran s'éteint au bout de deux minutes d'inactivité. Pour le réactiver, cliquez sur n'importe quel bouton.

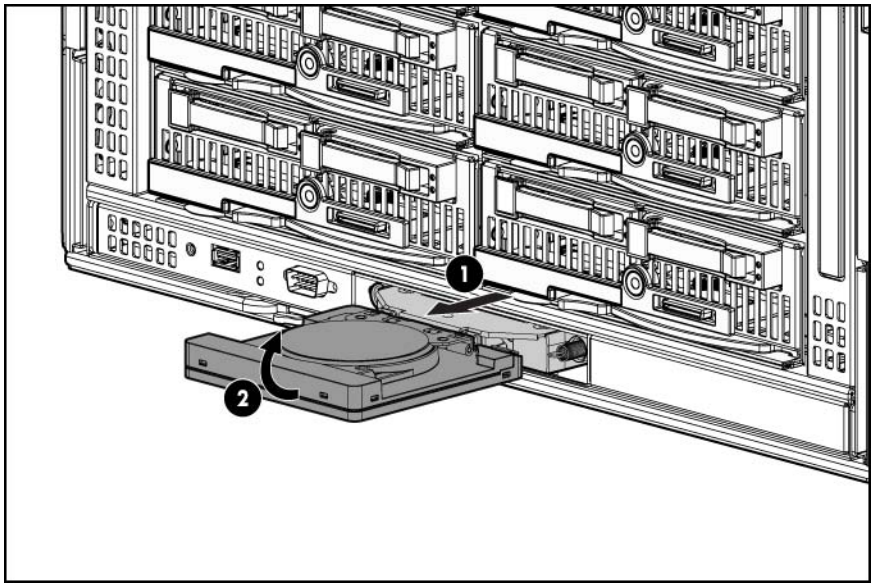
L'icône Enclosure Health (État du boîtier) située dans l'angle inférieur gauche de chaque écran indique la condition de l'état du boîtier. Déplacez le curseur sur l'icône Enclosure Health et cliquez sur OK pour accéder à l'écran Health Summary (Résumé d'intégrité) à partir de tout écran Insight Display.

Accès à l'écran HP BladeSystem c3000 Insight Display

1. Pour accéder au module Insight Display, appuyez sur l'extrémité exposée.



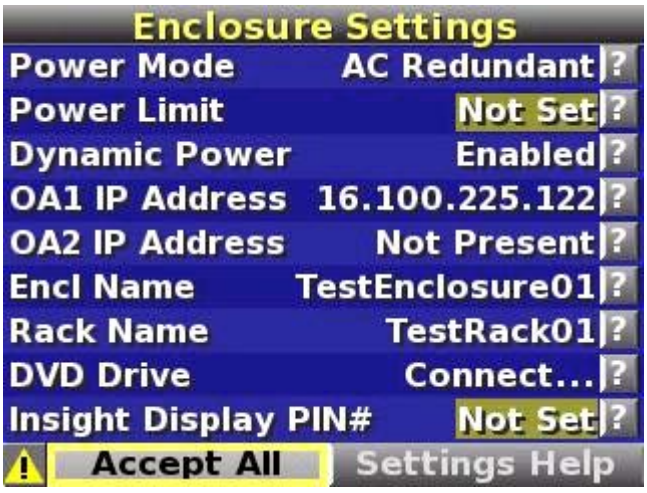
2. Tirez le module Insight Display hors du châssis afin de le verrouiller en place, puis inclinez-le.



Exécution de l'installation du module Insight Display

Pour identifier le boîtier, le voyant à l'arrière du boîtier et la partie arrière du module Insight Display s'illuminent en bleu lors de la première mise sous tension du boîtier. Lors de la première mise sous tension du boîtier, le module Insight Display lance un assistant d'installation pour vous guider pendant le processus de configuration. Au début de l'installation, l'assistant met automatiquement l'UID du boîtier sous tension. Une fois l'installation terminée, l'assistant met l'UID du boîtier hors tension. Après avoir configuré le boîtier, le module Insight Display vérifie qu'il n'y a aucune erreur de configuration ou d'installation. Si des erreurs sont présentes, le module Insight Display vous guide dans la procédure de correction des erreurs.

L'écran Enclosure Settings (Paramètres du boîtier) est le premier écran qui s'affiche.


Enclosure Settings
Power Mode AC Redundant ?
Power Limit Not Set ?
Dynamic Power Enabled ?
OA1 IP Address 16.100.225.122 ?
OA2 IP Address Not Present ?
Encl Name TestEnclosure01 ?
Rack Name TestRack01 ?
DVD Drive Connect... ?
Insight Display PIN# Not Set ?
Accept All
Settings Help

1. Passez en revue chaque paramètre de l'écran Enclosure Settings (Écran Enclosure Settings à la page 38) pour vérifier qu'il est correct.
2. Pour modifier une valeur, accédez à l'option de menu à modifier, puis appuyez sur le bouton **OK**.

3. Modifiez le paramètre sur la valeur appropriée, placez le curseur sur **Accept** (Accepter), puis appuyez sur le bouton **OK** pour revenir au menu Enclosure Settings (Paramètres du boîtier). Répétez cette opération jusqu'à ce que toutes les options du menu Enclosure Settings soient correctes.

ASTUCE : Sélectionnez l'icône ? pour accéder à des informations d'aide détaillées sur chaque paramètre ou chaque rubrique.

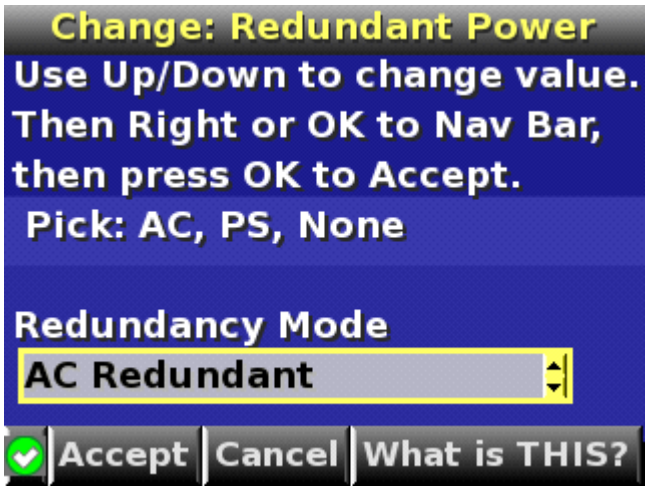
ASTUCE : Dans toute option de menu, placez le curseur sur **What is This** (Qu'est-ce que c'est), puis appuyez sur le bouton **OK** pour afficher des informations supplémentaires sur chaque paramètre, option ou alerte.

4. Une fois que tous les paramètres du menu Enclosure Settings vous conviennent, placez le curseur sur **Accept All** (Tout accepter), puis appuyez sur le bouton **OK** pour accepter les paramètres actuels.

   Vous pouvez modifier les options suivantes dans l'écran Enclosure Settings :

   Power Mode (Mode d'alimentation) : la valeur par défaut est AC Redundant (Redondance secteur). Les sélections suivantes sont valides :

   - AC Redundant (Redondance secteur)
   - Power Supply Redundant (Redondance d'alimentation)
   - None (Aucun)



   Power Limit (Seuil d'alimentation) : le paramètre par défaut est Not Set (Non défini). Vous pouvez modifier la limite par incréments de 50 Watts.

ATTENTION : Lors du calcul de la valeur Power Limit Watts AC, abaissez le circuit à 80 % du maximum pour empêcher le déclenchement du disjoncteur (États-Unis seulement).

ATTENTION : Si votre équipement n'est pas en mesure de supporter la valeur crête en watts CA calculée, réglez la valeur Power Watts AC afin de l'adapter aux capacités de votre équipement.

   Dynamic Power (Alimentation dynamique) : le paramètre par défaut est Disabled (Désactivé). Les sélections suivantes sont valides :

- **Enabled** (Activé) : certaines alimentations peuvent être automatiquement placées en veille pour augmenter l'efficacité globale du sous-système d'alimentation du boîtier.
- **Disabled** (Désactivé) : toutes les alimentations partagent la charge. L'efficacité du sous-système d'alimentation varie en fonction de la charge.

REMARQUE : L'alimentation dynamique est prise en charge avec tous les blocs d'alimentation c3000. Elle est prise en charge avec tous les blocs d'alimentation c7000, à l'exception de ceux fonctionnant avec une tension d'entrée basse (nominale 100-120 VCA).

OA1 IP Addr (Adresse IP OA1) : le paramètre par défaut est DHCP. Si aucune adresse IP n'est reçue, l'adresse IP est 0.0.0.0. L'adresse IP, le masque et la passerelle sont définis dans cette option.

OA2 IP Addr (Adresse IP OA2) : si ce module est présent, le paramètre par défaut est DHCP. Si aucune adresse IP n'est reçue, l'adresse IP est 0.0.0.0. Si un seul module Onboard Administrator est installé, l'écran affiche « Not Present » (Absent).

Enclosure Name (Nom de boîtier) : la valeur par défaut est un nom unique attribué en usine. Les valeurs caractères acceptées sont 0–9, A–Z, a–z, -, _ et □. Le □ symbole est utilisé pour indiquer la fin du nom.

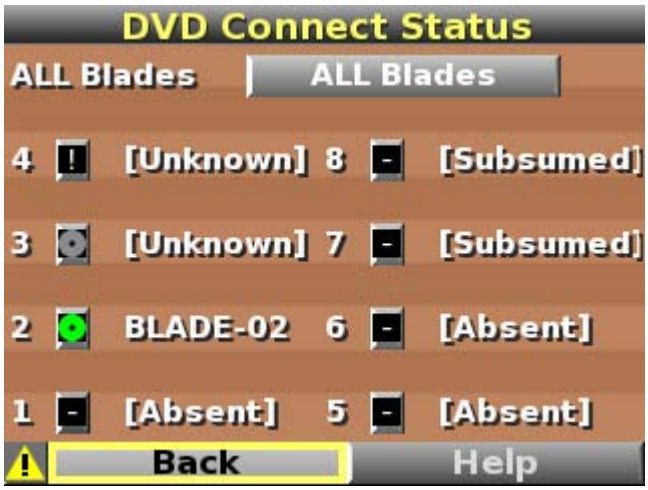
REMARQUE : N'utilisez pas le □ symbole au milieu d'un champ de texte. Les entrées dans les champs de texte sont tronquées au dernier caractère précédant le □ symbole.

ASTUCE : Sélectionnez **Clear** (Effacer) dans la barre de navigation pour effacer rapidement les entrées dans les champs de texte jusqu'au □ symbole.

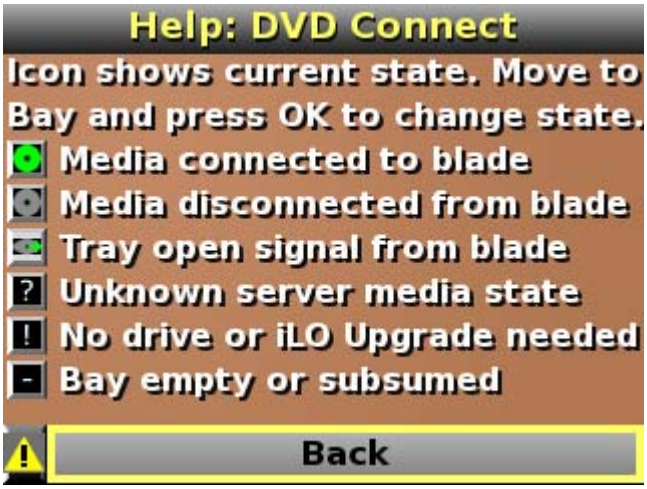
Rack Name (Nom de rack) : le paramètre par défaut est UnnamedRack. Les valeurs caractères acceptées sont 0–9, A–Z, a–z, -, _ et □. Le □ symbole est utilisé pour indiquer la fin du nom.

DVD Drive (Unité de DVD) : le paramètre par défaut est Disconnected (Déconnecté) sur toutes les lames. Le menu DVD Connect Status (État de connexion du DVD) affiche l'état de connexion actuel du DVD avec une icône.

Pour accéder au menu de connexion de DVD de lame, sélectionnez une icône de DVD dans le menu DVD Connect.



Pour afficher les diverses icônes DVD Connect et leur signification, cliquez sur Help (Aide).

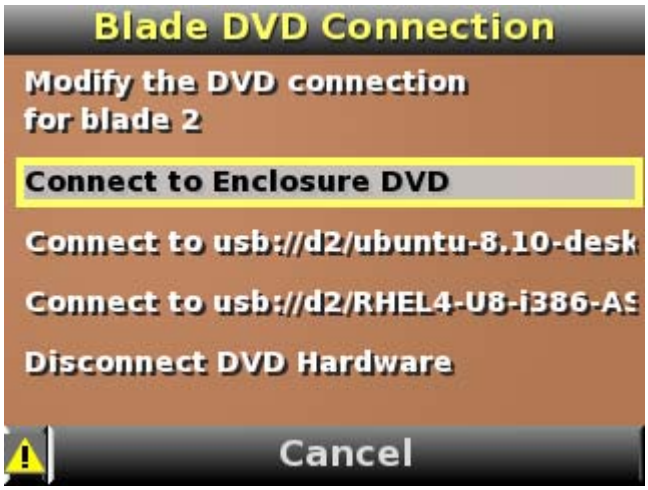

Help: DVD Connect
Icon shows current state. Move to
Bay and press OK to change state.
Media connected to blade
Media disconnected from blade
Tray open signal from blade
Unknown server media state
No drive or iLO Upgrade needed
Bay empty or subsumed
Back

Si le numéro de code PIN du module Insight Display est défini, le menu DVD Drive est protégé par le code PIN de l'écran LCD. Pour afficher ou modifier les paramètres de DVD du boîtier, vous devez saisir le code PIN correct sur l'écran LCD.

Pour connecter une lame à un CD, un DVD ou un fichier ISO, naviguez vers une icône de serveur individuel ou le bouton **All Blades** (Toutes les lames), puis cliquez sur **OK**.

Le menu Blade DVD Connection (Connexion de DVD de lame) indique si un DVD de boîtier ou un fichier ISO sur une clé USB est disponible pour établir une connexion à des serveurs sélectionnés sur le menu DVD Connect Status (État de connexion de DVD). Si plusieurs fichiers ISO sont trouvés sur la clé USB, il peut exister plus d'une page d'options. Pour afficher la page suivante d'options de connexion, sélectionnez le bouton **Page suivante**.

- **Connect to** (Connecter à) : sélectionnez une des options actuellement disponibles, puis cliquez sur **OK** pour sélectionner cette option et naviguez vers le menu **Connect: Blade DVD** (Connexion : DVD de lame) pour spécifier de redémarrer le serveur avec ce support connecté ou de laisser les serveurs dans l'état d'alimentation existant.
- **Disconnect DVD Hardware** (Déconnecter le matériel de DVD) : déconnecte la connexion du support actuel et revient au menu **DVD Connect Status** (État de connexion de DVD).



Les sélections suivantes sont valides :

- **No Power Change** (Pas de modification d'alimentation) : connecte le support sélectionné au serveur uniquement.

- **Connect and Reboot** (Connecter et redémarrer) : connecte le support sélectionné aux serveurs sélectionnés et redémarre ces derniers.

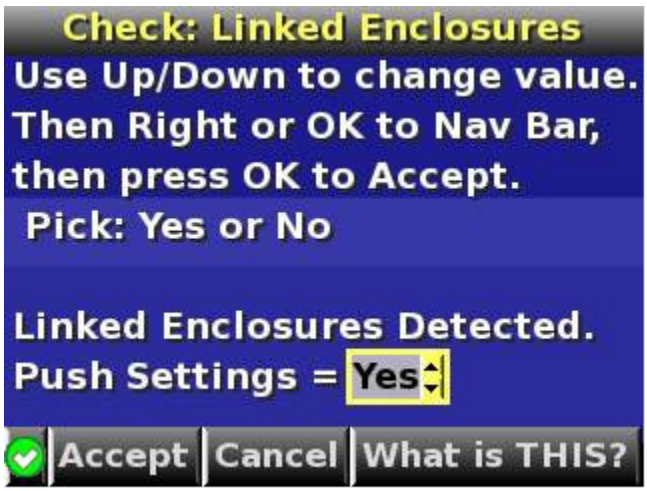
5. Pour accepter tous les paramètres et poursuivre, accédez au bouton **Accept All** (Tout accepter) en bas de l'écran Enclosure Settings, puis cliquez sur le bouton **OK**.

   Si le module Onboard Administrator détecte d'autres boîtiers, le message « Linked enclosures detected » (Boîtiers liés détectés) s'affiche.

6. Utilisez les boutons fléchés haut et bas pour modifier les paramètres **Push Settings =** (Paramètres Push) sur l'une des valeurs suivantes :

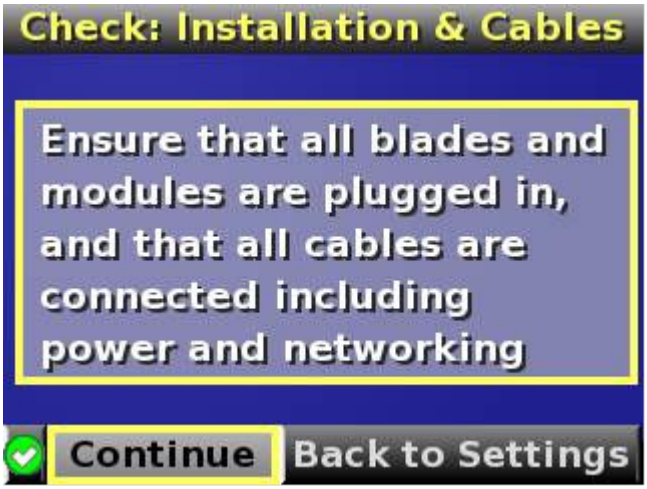
   - **Yes** (Oui) : copie sur les boîtiers détectés les paramètres d'alimentation configurés, le nom du rack et le code PIN de verrouillage LCD (s'il est défini) de l'écran Enclosure Settings.
   - **No** (Non) : continue la configuration du boîtier actuel uniquement. L'assistant d'installation du module Insight Display doit être exécuté sur chaque boîtier détecté. Choisissez cette option si chaque boîtier nécessite des paramètres d'alimentation différents.

   REMARQUE : Si votre installation utilise un adressage IP statique sur le module Onboard Administrator, vous devez entrer manuellement ces adresses IP dans Insight Display pour chaque module Insight Display séparément. Vous pouvez entrer ces adresses IP de module Onboard Administrator avant d'envoyer les paramètres aux boîtiers adjacents. Au besoin, vous pouvez revenir au menu Enclosure Settings une fois que l'assistant d'installation a terminé de modifier les adresses IP du module Onboard Administrator.



7. Positionnez le curseur sur **Accept** (Accepter), puis appuyez sur le bouton **OK**.

   L'assistant d'installation affiche l'écran Check: Installation & Cables (Contrôle : Installation et Câbles).

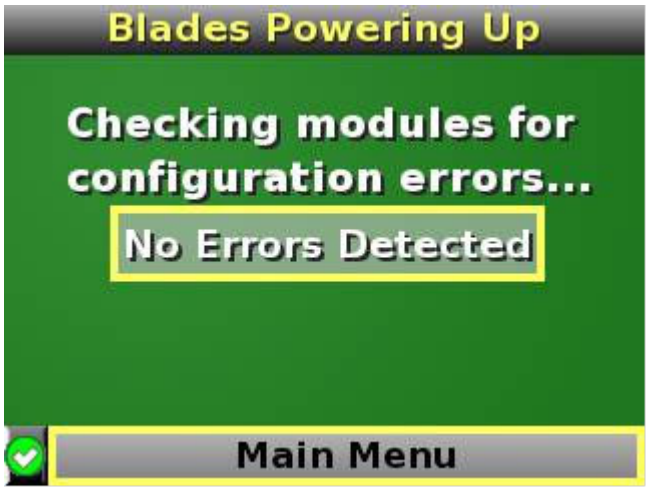

Check: Installation & Cables
Ensure that all blades and modules are plugged in, and that all cables are connected including power and networking
Continue
Back to Settings

8. Vérifiez que tous les composants sont installés et connectés.
9. Pour commencer la vérification des erreurs d'installation et de configuration, sélectionnez **Continue**, puis appuyez sur **OK**. Lorsque **Continue** est sélectionné, l'identification d'unité (UID) du boîtier se désactive automatiquement. Si **Push Settings = Yes** :

   - Les paramètres du boîtier sont passés aux boîtiers adjacents.
   - L'assistant d'installation s'exécute sur chaque boîtier adjacent.
   - L'identification d'unité du boîtier se désactive sur les boîtiers adjacents.

   Si aucune erreur n'est détectée, l'identification d'unité arrière du boîtier se désactive et l'écran Insight Display s'allume en vert.

10. Pour revenir au menu principal, appuyez sur **OK**. L'installation et la configuration du boîtier et du matériel de lame sont terminées.



REMARQUE : Si des erreurs sont détectées, l'écran Insight Display s'allume en orange et l'écran Health Summary (Résumé d'intégrité) s'affiche. Pour plus d'informations sur la résolution d'erreurs d'installation et de configuration, reportez-vous à la section « Erreurs du module Insight Display » (Erreurs du module Insight Display à la page 46).

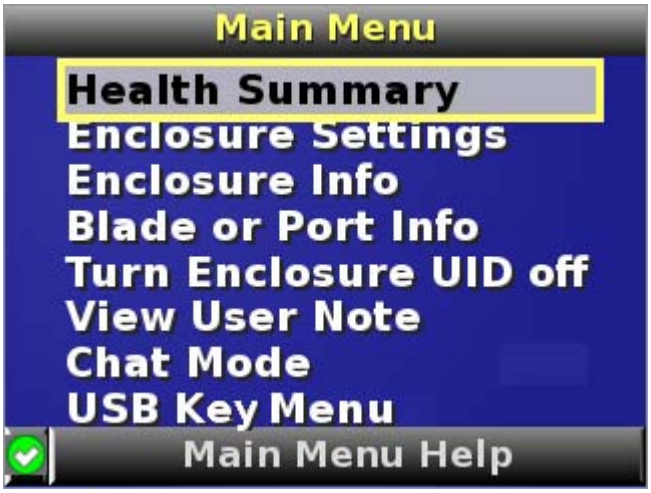
Toutes les erreurs de configuration interdisent le fonctionnement du boîtier et doivent être corrigées immédiatement.

11. Ouvrez un navigateur et connectez-vous au module Onboard Administrator actif à l'aide de l'adresse IP Onboard Administrator qui a été configurée lors de l'exécution de l'assistant d'installation de l'écran Insight Display.
12. Saisissez le nom d'utilisateur et le mot de passe correspondant au module Onboard Administrator pour accéder à l'interface Web Onboard Administrator distante, puis exécutez l'assistant d'installation Onboard Administrator qui apparaît lors du premier accès.

Navigation dans le module Insight Display

Vous pouvez naviguer dans les menus et sélections à l'aide des boutons fléchés de l'écran Insight Display.

Le premier menu qui s'affiche est le menu principal :

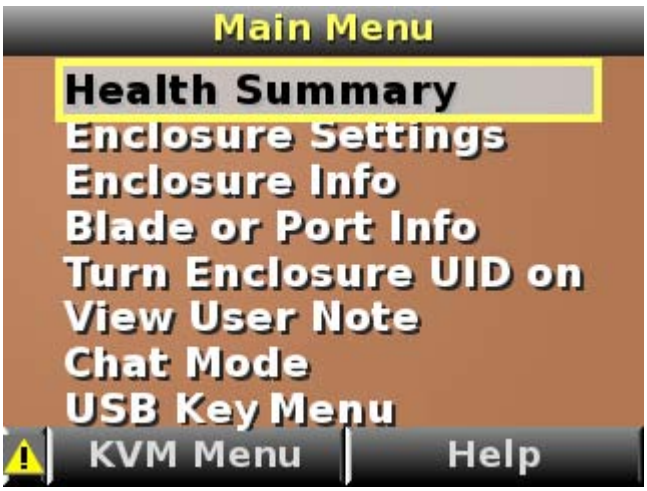


Le menu principal du module Insight Display comporte les options de menu suivantes :

- Health Summary (Résumé d'intégrité)
- Enclosure Settings (Paramètres du boîtier)
- Enclosure Info (Informations de boîtier)
- Blade and Port Info (Informations de lame et de port)
- Turn Enclosure UID On/Off (Activer/désactiver l'identification d'unité du boîtier)
- View User Note (Afficher la note de l'utilisateur)
- Chat Mode (Mode Conversation)
- Menu USB Key (Clé USB)

Si le module Onboard Administrator actif détecte la fonction KVM, un bouton de menu KVM apparaît sur la barre de navigation dans le menu principal. La sélection du menu KVM entraîne l'effacement de toutes les données sur l'écran Insight Display et active la connexion VGA du module Onboard Administrator.

La fonction KVM figure dans l'image de menu principal suivante.



Pour plus d'informations sur le menu principal de l'écran Insight Display, consultez le *Manuel de l'utilisateur de HP BladeSystem Insight Display*.

ASTUCE : Dans toute option de menu, placez le curseur sur **What is This** (Qu'est-ce que c'est), puis appuyez sur le bouton **OK** pour afficher des informations supplémentaires sur chaque paramètre, option ou alerte.

La barre de navigation contient des options pour :

- Naviguer vers l'avant et l'arrière dans les écrans d'alerte
- Revenir au menu principal
- Accepter les modifications apportées aux paramètres en cours
- Annuler les modifications apportées aux paramètres en cours
- Accéder à l'écran Health Summary depuis n'importe quel écran en sélectionnant l'icône Health Summary sur la barre de navigation

Écran Health Summary

L'écran Health Summary affiche la condition actuelle du boîtier. Pour accéder à l'écran Health Summary (Résumé d'intégrité) :

- Sélectionnez **Health Summary** dans le menu principal
- Sélectionnez l'icône **Health Summary** dans tout écran Insight Display

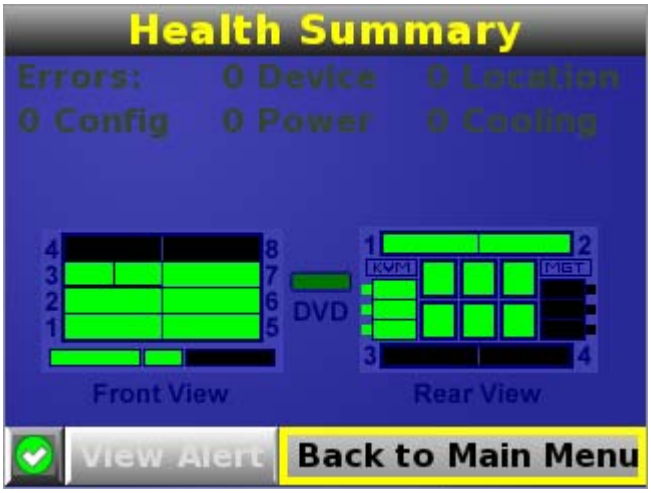
Lorsqu'une condition d'erreur ou d'alerte est détectée, l'écran Health Summary affiche le nombre total de conditions d'erreur et les emplacements de ces erreurs.

Sélectionnez **Next Alert** (Alerte suivante) dans la barre de navigation, puis appuyez sur le bouton **OK** pour afficher chaque condition d'erreur individuelle. Le module Insight Display affiche chaque condition d'erreur par ordre de gravité. Les alertes critiques s'affichent en premier (le cas échéant), suivies des alertes demandant l'attention de l'utilisateur.

Lorsque le boîtier fonctionne normalement, l'écran Health Summary s'affiche en vert. Les rectangles en vert intense sont les éléments installés et en service. Un rectangle vert foncé représente un élément qui est installé mais mis hors tension sans erreur. Un rectangle noir désigne une baie vide.

Remarque : dans le cas de la fonction c-Class Enclosure DVD (DVD de boîtier c-Class), un rectangle de DVD noir indique qu'aucun lecteur de DVD n'est connecté au module Onboard Administrator alors qu'un rectangle gris foncé indique que le lecteur de DVD est présent mais qu'aucun support n'est présent. Un rectangle vert foncé indique que le support est présent mais non activement connecté à tout serveur ou que tous les serveurs connectés ont émis une commande d'éjection de disque, afin que le disque puisse être retiré de l'unité. Un rectangle vert intense indique que le support est présent dans l'unité et activement connecté à au moins un serveur dans le boîtier, et le plateau de l'unité est verrouillé.

Si une erreur est présente, la couleur d'arrière-plan de l'écran Health Summary change du vert à l'orange et l'erreur est mise en surbrillance avec des rectangles jaunes pour attention et des rectangles rouges pour échecs. Les icônes d'état global du boîtier dans l'angle inférieur gauche de tous les écrans Insight Display indiquent l'état global du boîtier.



Sélectionnez **View Alert** (Afficher l'alerte), puis appuyez sur le bouton OK pour afficher les erreurs.

Sélectionnez **Details** (Détails) pour afficher les détails de l'erreur.

Écran Enclosure Settings

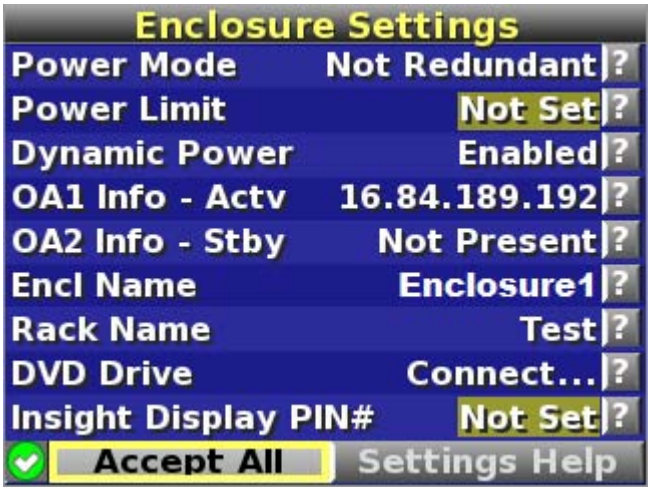
L'écran Enclosure Settings affiche les informations de paramétrage suivantes sur le boîtier :

- Paramètre Power Mode (Mode d'alimentation)
- Paramètre Power Limit (Seuil d'alimentation)
- Paramètre Dynamic Power (Alimentation dynamique)
- Adresse IP OA active et de réserve
- Enclosure name (Nom du boîtier)
- Rack Name (Nom du rack)
- DVD Drive (Lecteur de CD/DVD-ROM)
- PIN Insight Display

REMARQUE : Le paramètre DVD Drive peut connecter ou déconnecter un CD ou DVD chargé dans le lecteur de DVD optionnel du boîtier c3000 par rapport à n'importe quelle ou toutes les lames de serveur du boîtier. Cette fonctionnalité permet d'installer un système d'exploitation ou logiciel sur les lames de serveur. Si le lecteur de DVD optionnel n'est pas présent, un lecteur de DVD USB HP externe peut être utilisé avec cette fonction.

ASTUCE : Définissez un code PIN pour protéger les paramètres du boîtier contre toute modification.

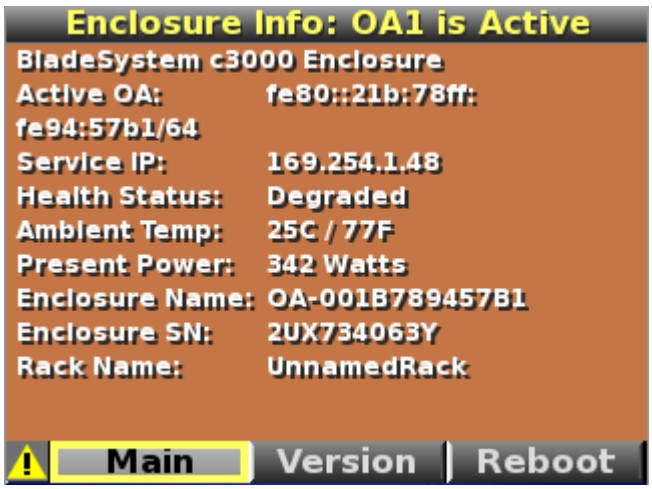
Positionnez le curseur sur un paramètre ou sur le signe ?, puis appuyez sur OK pour modifier le paramètre ou obtenir de l'aide sur ce dernier.



Écran Enclosure Info

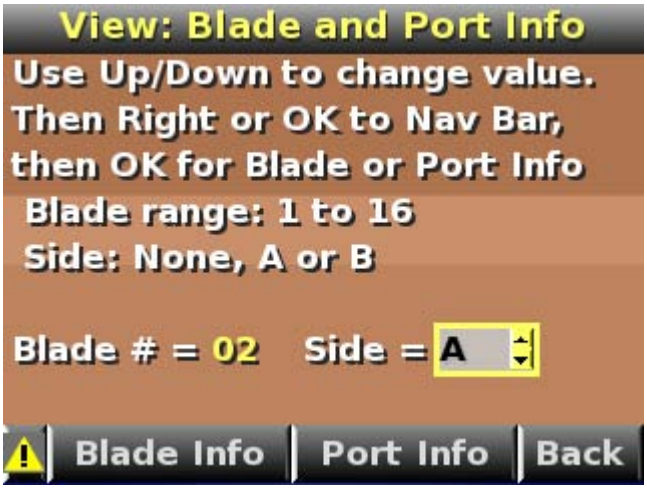
L'écran Enclosure Info affiche des informations sur le boîtier, notamment :

- Adresse IP OA active
- Adresse IP de service active
- État d'intégrité actuel
- Température ambiante actuelle
- Tension d'entrée CA actuelle
- Nom
- Numéro de série
- Nom du rack



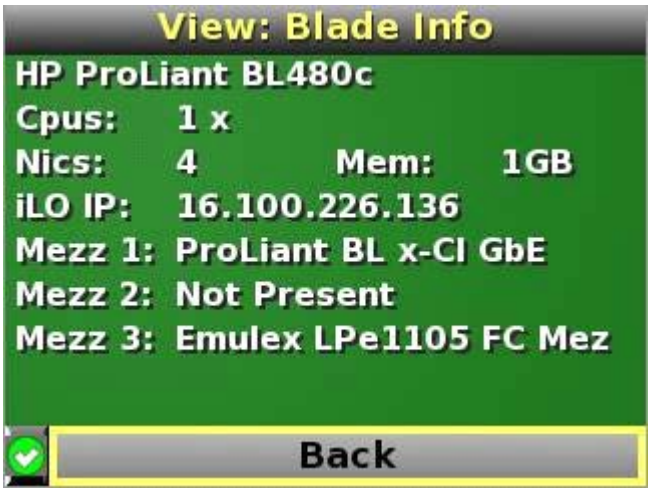
Écran Blade and Port Info

L'écran Blade and Port Info (Informations de lame et de port) affiche des informations sur une lame de serveur spécifique. Sur le premier écran, sélectionnez le numéro de lame de serveur, puis appuyez sur le bouton OK. Sélectionnez **Blade Info** ou **Port Info**, puis appuyez sur le bouton OK.


View: Blade and Port Info
Use Up/Down to change value.
Then Right or OK to Nav Bar,
then OK for Blade or Port Info
Blade range: 1 to 16
Side: None, A or B
Blade # = 02
Side = A
Blade Info
Port Info
Back

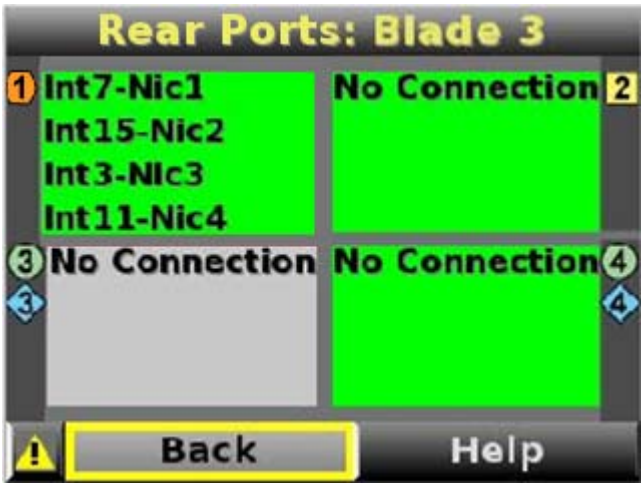
Lors de l'affichage d'un serveur BL2x220c, naviguez jusqu'à la deuxième zone de sélection et utilisez le bouton pointant vers le haut ou le bas pour sélectionner le serveur A ou B. La sélection correcte doit être N/A pour sélectionner tous les autres écrans d'informations de la lame de serveur.

Pour afficher des informations sur la lame de serveur, sélectionnez **Blade Info**, puis appuyez sur le bouton OK.



Pour afficher les ports utilisés par une lame de serveur spécifique, sélectionnez **Port Info**, puis appuyez sur le bouton OK.

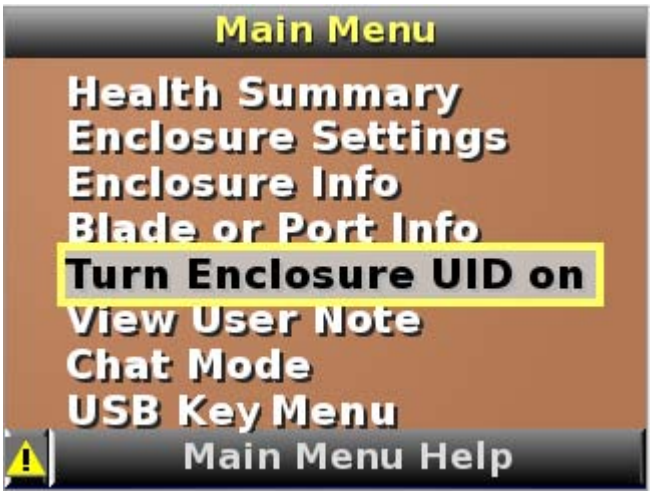
La lame de serveur pleine hauteur illustrée ci-dessous comporte quatre cartes réseau intégrées. Les autres baies d'interconnexion sont vides. Les quatre cartes réseau intégrées sont connectées à des numéros de port particuliers sur les modules d'interconnexion.



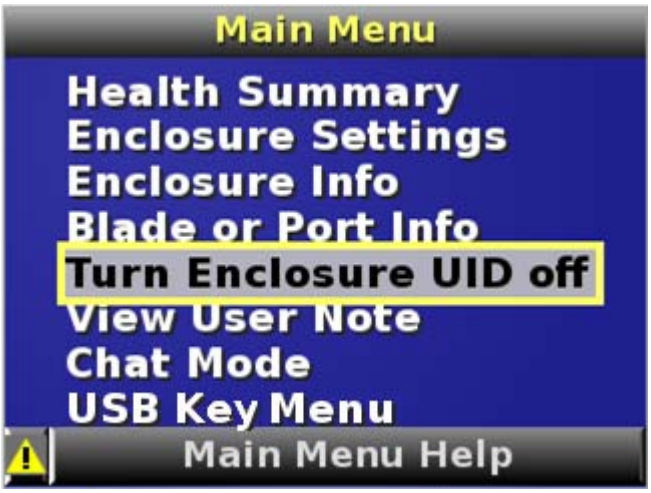
Écran Turn Enclosure UID On/Off

L'option du menu principal affiche « Turn Enclosure UID Off » (Désactiver l'identification d'unité du boîtier) lorsque l'identification d'unité du boîtier est active, et affiche « Turn Enclosure UID On » (Activer l'identification d'unité du boîtier) lorsque l'identification d'unité du boîtier est désactivée.

La sélection de **Turn Enclosure UID On** (Activer l'identification d'unité du boîtier) dans le menu principal allume le voyant arrière d'identification d'unité du boîtier et change la couleur de l'écran Insight Display en bleu.

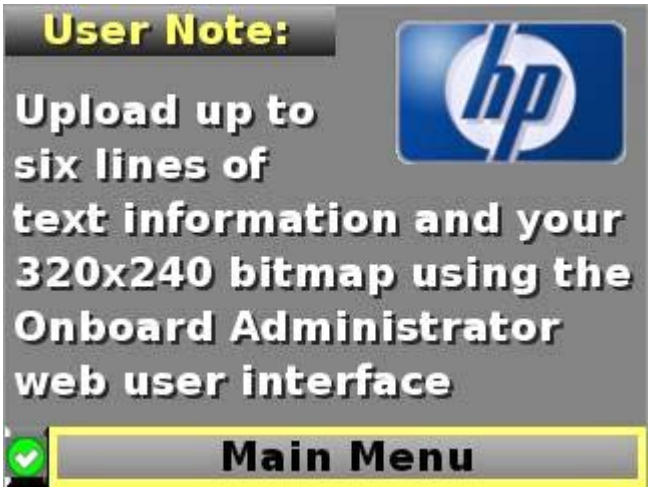


Lorsque vous sélectionnez **Turn Enclosure UID Off** (Désactiver l'identification d'unité du boîtier) dans le menu principal, le voyant UID du boîtier arrière s'éteint et l'écran Insight Display reprend une couleur de condition normale.



Écran View User Note

L'écran View User Note (Afficher la note de l'utilisateur) affiche six lignes de texte, chacune contenant un maximum de 25 caractères. Utilisez cet écran pour afficher des informations utiles, telles que des numéros de téléphone de contacts ou d'autres informations. Modifiez cet écran à l'aide de l'interface Web utilisateur distante du module Onboard Administrator. L'image bitmap d'arrière-plan et le texte peuvent être modifiés.


User Note:
Upload up to six lines of text information and your 320x240 bitmap using the Onboard Administrator web user interface
Main Menu

Écran Chat Mode

L'écran Chat Mode (Mode conversation) est utilisé par l'administrateur distant qui emploie l'interface Web pour envoyer un message à un module Insight Display d'un boîtier. Le technicien utilise les boutons de l'écran Insight Display pour effectuer une sélection dans un ensemble de réponses préparées, ou compose un message de réponse personnalisé sur la ligne ?. Pour envoyer une réponse à l'administrateur, positionnez le curseur sur **Send** (Envoyer), puis appuyez sur le bouton **OK**.

L'écran Chat Mode a priorité dans le module Insight Display et est maintenu jusqu'à ce que **Send** soit sélectionné. Le technicien peut quitter cet écran de conversation temporairement et utiliser les autres écrans de l'écran Insight Display, puis revenir à l'écran Chat Mode à partir du menu principal pour envoyer une réponse. Après la réponse, l'écran Chat Mode est effacé. Les réponses A et ? sont ensuite affichées par l'administrateur distant sur l'interface Web pour la conversation sur écran.

Écran USB Menu

Onboard Administrator (versions de microprogramme 2.30 et ultérieures) propose une prise en charge supplémentaire pour les options de clé USB suivantes :

- Mise à jour du microprogramme OA (à partir d'une image ISO HP SPP prise en charge)
- Restauration de configuration de module OA
- Enregistrement de configuration de module OA

Onboard Administrator prend en charge les clés USB formatées avec des systèmes de fichiers FAT32 ou ext2. La taille maximale de fichier prise en charge pour les clés USB formatées avec FAT32 est de 4 Go. Pour les images SPP supérieures à 4 Go, utilisez une clé USB de format ext2. La procédure de formatage de votre clé USB avec un système de fichiers ext2 est incluse à la fin de cette section.

Vous pouvez insérer une clé USB dans le port situé sur le module Onboard Administrator actif à l'avant du boîtier ou un port USB sur le module KVM facultatif.

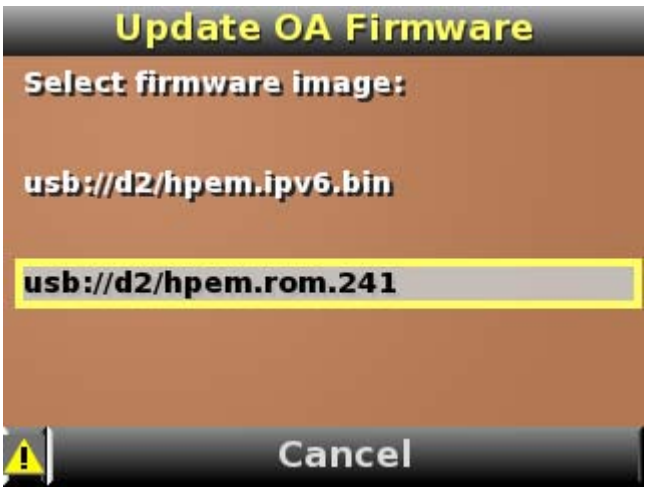
Pour accéder au menu USB Key :

1. Insérez une clé USB dans le module Onboard Administrator ou dans le module KVM facultatif.
2. Dans le menu principal, sélectionnez **USB Key Menu** (Menu Clé USB).

Les sélections suivantes sont disponibles sur le menu USB Key :

- **Update OA Firmware** (Mettre à jour le microprogramme OA) : sélectionnez cette option pour mettre à niveau le microprogramme. La clé USB doit contenir une image du microprogramme Onboard Administrator avec une extension de fichier BIN.

  Pour plus d'informations sur la mise à niveau de modules Onboard Administrator dans les boîtiers HP BladeSystem c3000 et c7000, consultez la section « Mise à niveau de modules Onboard Administrator dans un boîtier HP BladeSystem » (Mise à niveau de modules Onboard Administrator dans un boîtier HP BladeSystem à la page 224).



- **Restore Configuration** (Restaurer la configuration) : sélectionnez cette option pour télécharger un fichier de configuration de boîtier avec l'extension .CFG.

  Le menu Restore OA Configuration (Restauration de configuration OA) répertorie tous les fichiers sur la clé USB reliée avec une extension de fichier .CFG. Sélectionnez le fichier de configuration souhaité, puis appuyez sur **OK**.

  Dans la mesure où le fichier de configuration peut modifier des paramètres tels que l'adresse IP du module Onboard Administrator, veillez à uniquement appliquer le même fichier à plusieurs boîtiers si les paramètres sont génériques, telles que des adresses de serveur SNMP ou LDAP. N'appliquez pas le même fichier à plusieurs boîtiers s'il contient des commandes de configuration d'adresse IP de module Onboard Administrator ou des commandes d'adresse IP EBIPA.

- **Save Configuration** (Enregistrer la configuration) : sélectionnez cette option pour enregistrer la configuration du fichier dans un fichier sur la clé USB.

Formatage de votre clé USB avec un système de fichiers ext2, à partir d'un PC Windows

Avant de formater la clé USB, vous devez activer la prise en charge des systèmes de fichiers ext2 sur votre système Windows :

1. Téléchargez un fichier `Ext2Fsd-x.xx.exe` à partir du site Web SourceForge (http://sourceforge.net/projects/ext2fsd/).
2. Installez le fichier exécutable téléchargé.

Une fois ces étapes initiales terminées, votre système Windows doit être en mesure de reconnaître des clés USB au format ext2 et permettre d'y écrire des données.

Pour formater votre clé USB :

1. Téléchargez l'image ISO du CD Live Gparted depuis le site Web GNOME Partition Editor (http://gparted.org/). Le nom de l'image ISO est généralement au format `gparted-live-x.xx.x-x-i586.iso`.
2. Téléchargez un lecteur de machine virtuelle de votre choix et installez-le sur votre système Windows. Par exemple, installez le lecteur VMware disponible sur le site Web VMware (https://my.vmware.com/web/vmware/downloads).
3. Insérez la clé USB dans votre PC.

4. À l'aide de votre lecteur de machine virtuelle, créez une machine virtuelle avec un noyau Linux configurée avec les valeurs par défaut. (La version Linux du noyau doit être en conformité avec la distribution de Linux fournie par le CD Gparted Live.)
5. Définissez l'image ISO du CD Gparted Live en tant qu'option CD/DVD pour votre machine virtuelle, puis démarrez cette dernière.
6. Pour formater votre clé USB en ext2, utilisez les options appropriées de l'interface utilisateur sur la machine virtuelle Gparted.
7. Retirez la clé USB de la machine virtuelle.
8. Mettez hors tension la machine virtuelle à partir du lecteur de machine virtuelle.
9. Pour confirmer que la clé USB est désormais formatée en ext2, vérifiez-en les propriétés à partir de votre PC.

Copiez l'image ISO de SPP sur la clé USB.

1. Installez les drivers de système de fichiers ext2 pour Windows. Les drivers se trouvent sur le site Web SourceForge (http://sourceforge.net/projects/ext2fsd/).
2. Vos systèmes Windows devraient désormais détecter la clé USB au format ext2.
3. Chargez l'image ISO de SPP sur la clé USB.

Écran KVM Menu

Si la fonction Enclosure KVM est prise en charge, le menu principal Insight Display affiche un bouton **KVM Menu**. Sélectionnez ce bouton pour désactiver le module Insight Display et activer le connecteur VGA sur le module KVM. Une seule des deux interfaces peut être active à la fois. Pour plus d'informations, reportez-vous à la section « KVM de boîtier » (Boîtier KVM à la page 49).

Erreurs du module Insight Display

L'installation du boîtier a réussi lorsque toutes les erreurs sont corrigées. Les erreurs dans les sections suivantes sont spécifiques à l'installation et à la configuration initiale du boîtier. Pour éliminer les erreurs qui se produisent après la mise sous tension et la configuration initiales, consultez le *Manuel de l'utilisateur du module HP BladeSystem Onboard Administrator* pour plus d'informations.

Les types d'erreurs suivants peuvent se produire lors de l'installation et de la configuration du boîtier :

- Erreurs d'alimentation (Erreurs d'alimentation à la page 47)
- Erreurs de refroidissement (Erreurs de refroidissement à la page 47)
- Erreurs d'emplacement (Erreurs d'emplacement à la page 47)
- Erreurs de configuration (Erreurs de configuration à la page 47)
- Erreur de panne de périphérique (Erreur de panne de périphérique à la page 48)

Lorsque le voyant d'identification d'unité du boîtier est éteint, le module Insight Display est allumé en orange en présence d'une condition d'erreur. La barre de navigation affiche les sélections suivantes en présence d'une condition d'erreur :

- Icône Health Summary (Résumé d'intégrité) : affiche l'écran Health Summary (Résumé d'intégrité).
- Fix THIS (Réparer CECI) : suggère des actions correctives pour éliminer l'erreur actuelle.

- Next Alert (Alerte suivante) : affiche l'alerte suivante ou, en l'absence d'alerte, affiche l'écran Health Summary (Résumé d'intégrité).
- Previous Alert (Alerte précédente) : affiche l'alerte précédente.

Erreurs d'alimentation

Des erreurs d'alimentation peuvent se produire en cas d'alimentation insuffisante pour mettre un boîtier en service. Des erreurs d'alimentation peuvent se produire sur des lames de serveur, des lames de stockage ou des modules d'interconnexion.

Pour corriger une erreur d'alimentation :

1. Utilisez les boutons fléchés pour accéder à **Fix This** (Corriger ceci), puis appuyez sur **OK**.
2. Lisez et exécutez l'action corrective suggérée par le module Insight Display. Dans la plupart des cas, vous devez ajouter des alimentations au boîtier ou retirer les éléments indiqués.

Erreurs de refroidissement

Les erreurs de ventilation se produisent lorsque le nombre de ventilateurs installés dans le boîtier est insuffisant ou lorsque les ventilateurs existants ne sont pas installés selon une configuration efficace. Des erreurs de refroidissement peuvent se produire sur des lames de serveur, des lames de stockage ou des modules d'interconnexion.

Pour corriger une erreur de refroidissement :

1. Utilisez les boutons fléchés pour accéder à **Fix This** (Corriger ceci), puis appuyez sur **OK**.
2. Lisez et exécutez l'action corrective suggérée par le module Insight Display. Dans la plupart des cas, vous devez ajouter des ventilateurs au boîtier, corriger la configuration des ventilateurs ou retirer les éléments indiqués.

Erreurs d'emplacement

Les erreurs d'emplacement (installation) se produisent lorsque l'élément n'est pas installé dans la baie appropriée. Les erreurs d'emplacement peuvent se produire sur des lames de serveur, des lames de stockage ou des modules d'interconnexion.

Pour corriger une erreur d'emplacement :

1. Utilisez les boutons fléchés pour accéder à **Fix This** (Corriger ceci), puis appuyez sur **OK**.
2. Lisez et exécutez l'action corrective suggérée par le module Insight Display. Retirez l'élément indiqué, puis installez-le dans la baie appropriée. Le module Insight Display indique le numéro de baie approprié.

Erreurs de configuration

Les erreurs de configuration peuvent se produire si les modules d'interconnexion sont installés dans des baies inappropriées ou si des cartes mezzanine sont installées dans les mauvais connecteurs dans la lame de serveur. Des erreurs de configuration peuvent se produire sur des lames de serveur et des modules d'interconnexion.

Pour corriger une erreur de configuration :

1. Utilisez les boutons fléchés pour accéder à **Fix This** (Corriger ceci), puis appuyez sur **OK**.
2. Lisez et exécutez l'action corrective suggérée par le module Insight Display. Selon l'erreur reçue, effectuez l'une des interventions suivantes :

- Retirez le module d'interconnexion indiqué, puis installez-le dans la baie appropriée (le module Insight Display indique la baie appropriée).
- Retirez la lame de serveur pour corriger l'installation de la carte mezzanine (le module Insight Display indique la baie appropriée). Pour obtenir des informations sur l'installation de la carte mezzanine, reportez-vous au manuel de l'utilisateur spécifique du serveur sur le CD Documentation.

Erreur de panne de périphérique

Les erreurs de panne de périphérique se produisent lorsqu'un élément subit une défaillance. Des erreurs de panne de périphérique peuvent se produire sur tous les éléments, notamment :

- Lames de serveur
- Lames de stockage
- Alimentations
- Modules d'interconnexion
- Modules Onboard Administrator
- Ventilateurs
- Entrées d'alimentation secteur

Pour corriger une erreur de panne de périphérique :

1. Utilisez les boutons fléchés pour accéder à **Fix This** (Corriger ceci), puis appuyez sur **OK**.
2. Lisez et exécutez l'action corrective suggérée par le module Insight Display. Dans la plupart des cas, vous devez retirer l'élément concerné pour éliminer l'erreur.
3. Remplacez l'élément concerné par une pièce de rechange, si applicable.

REMARQUE : Si l'erreur de panne de périphérique est une erreur de panne d'entrée d'alimentation secteur, il convient de faire réparer l'entrée secteur défaillante pour éliminer l'erreur.

4 Boîtier KVM

Fonctionnalités

La fonction Enclosure KVM (KVM de boîtier) permet au module Onboard Administrator de passer d'une console vidéo de serveur à une autre en utilisant seulement un moniteur VGA attaché, un clavier USB et une souris USB, sans nécessiter un PC. En plus de lancer et d'exécuter des consoles vidéo de serveur, le menu Enclosure KVM (KVM de boîtier) fournit l'état d'intégrité de chaque serveur et permet à l'utilisateur d'activer et de désactiver l'alimentation des serveurs et de relier le DVD du boîtier à ces serveurs.

L'écran Insight Display est désactivé (écran vide) lorsque le menu Enclosure KVM est actif. Le menu Enclosure KVM (KVM de boîtier) inclut un bouton permettant d'accéder aux écrans Insight Display sur le moniteur VGA à l'aide des touches de curseur du clavier.

Le menu Enclosure KVM comprend également un bouton pour sélectionner la console de l'interface CLI du module Onboard Administrator. Après la connexion à la console de l'interface CLI du module Onboard Administrator à l'aide de l'option Enclosure KVM, l'utilisateur peut accéder à toutes les fonctions CLI.

Pour le boîtier c3000, la fonctionnalité KVM nécessite l'installation du module KVM facultatif à l'arrière du boîtier. Ce module KVM fournit un connecteur VGA et deux connecteurs supplémentaires USB 2.0. Pour le boîtier c7000, cette fonctionnalité nécessite le module Onboard Administrator avec le connecteur VGA.

Méthodes d'utilisation de la fonctionnalité Enclosure KVM

Pour utiliser la fonctionnalité Enclosure KVM, choisissez l'une des méthodes suivantes :

- Connectez directement le connecteur VGA à un moniteur VGA, puis connectez un clavier et une souris aux connecteurs USB.
- Connectez le connecteur VGA à un interrupteur KVM HP à l'aide d'un adaptateur CAT5 KVM USB, puis connectez le câble USB de l'adaptateur au connecteur USB du module Onboard Administrator.

REMARQUE : Si des problèmes de répétition de caractères se produisent lors de la saisie dans une console texte graphique sur un système Linux, les paramètres de configuration suivants peuvent nécessiter une modification :

Définissez le paramètre de répétition/délai du clavier sur 1 000 ms (kbdrate –d 1 000 dans le script d'initiation du serveur).

Configurez le taux de répétition auto de l'interface GUI sur 1 seconde.

Accès au menu KVM

Accédez au menu KVM en choisissant une des options suivantes :

- À partir d'un clavier USB connecté au module KVM, appuyez sur **Impr écran** ou **SysReq**.
- À partir d'un moniteur VGA avec un clavier et une souris, appuyez sur **Impr écran**.
- Si le module KVM est connecté à un commutateur KVM de rack HP à l'aide d'une carte VGA ou USB, appuyez sur **Impr écran** pour activer le menu de sélection KVM de rack HP, puis appuyez à nouveau sur **Impr écran** pour afficher le menu Enclosure KVM.

Sélectionnez le port KVM du rack HP connecté au boîtier, puis appuyez sur la touche **Entrée** pour sélectionner le menu Enclosure KVM. Si l'écran est vierge, touchez une touche quelconque du clavier pour activer le menu KVM et désactiver le module Insight Display du boîtier.

L'écran Insight Display apparaît vierge lorsque le menu Enclosure KVM est actif.

Retour au menu KVM à partir d'une autre interface

Pour revenir au menu KVM à partir d'une console de serveur, de l'écran Insight Display ou de l'affichage de l'interface OA, appuyez sur la touche **Impr écran** sur le clavier USB.

Retour à Insight Display à partir du menu KVM

Pour restaurer l'écran Insight Display et effacer le menu KVM (un léger délai peut se produire), appuyez sur tout bouton de l'écran Insight Display ou sélectionnez **Exit KVM** (Quitter KVM) dans le menu KVM.

Navigation dans le menu KVM

Le schéma suivant illustre le menu KVM :

HP KVM Menu Enclosure: c3000-E05 Rack: CT001
Press Sys Rq or Prt Sc key to return to this KVM Menu from other screens.
If you are also using an HP KVM switch, you have to press Prt Sc twice.
Status Bay# - Server Name
1 - YOUR-ESFCNZWOXG
2 - ORACLE-006
3 - ORACLE-007
4 - EXCHANGE-2
5 - ORACLE-009
6 - DHCP2
7 - LICENSE-SRV1
8 - CITRIX-1-24
Insight Display
OA CLI Console
Exit KVM
HELP

Pour naviguer dans le menu HP KVM, utilisez les touches fléchées du clavier. Pour sélectionner une action de menu, appuyez sur la touche **Entrée** du clavier.

Les actions disponibles incluent :

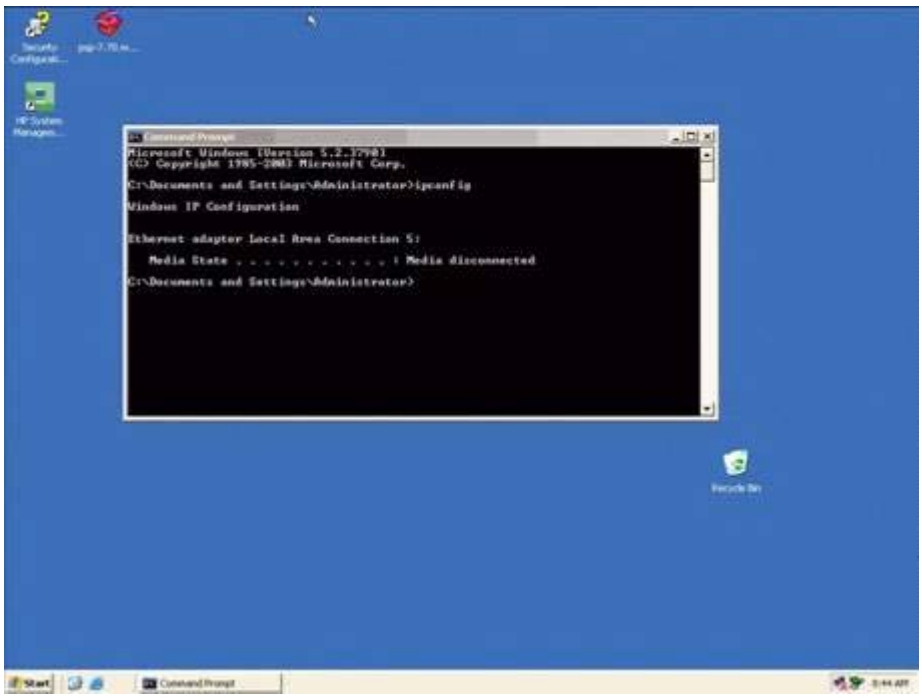
- Icône d'alimentation : modifie l'état d'alimentation du serveur.
- Icône de DVD : modifie l'état de DVD de boîtier du serveur.
- Nom du serveur : permet de se connecter à la console KVM plein écran du serveur, notamment prise en charge du clavier et de la souris. Pour revenir au menu KVM, appuyez sur la touche **Impr écran** ou **SysRq**.
- Insight Display : utilise le moniteur KVM et les touches fléchées et **Entrée** du clavier pour exploiter l'écran Insight Display.
- Console CLI OA : utilise le moniteur KVM et le clavier pour accéder aux commandes CLI OA.

- Quitter KVM : désactive le moniteur KVM et active l'écran Insight Display du boîtier.
- Aide : affiche un écran d'aide HP KVM comportant des informations sur les icônes d'état et le fonctionnement KVM.

Si le code PIN de l'écran LCD est défini, toutes les commandes d'alimentation et de DVD du serveur sont protégées par le code PIN de l'écran. La console du serveur et l'interface de ligne de commande du module Onboard Administrator sont protégées par les connexions utilisateur.

Le menu KVM contient les options suivantes :

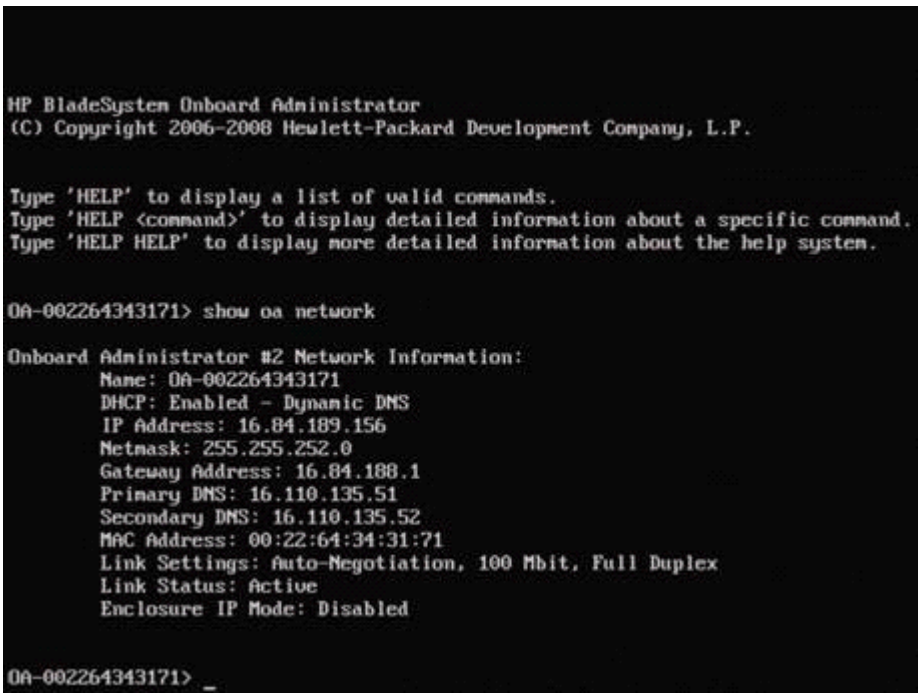
- Server Console (Console de serveur) : sélectionnez une console de serveur en sélectionnant le nom du serveur. La console de serveur sélectionnée est une console graphique plein écran ou texte sur la base de l'environnement actuel sur ce serveur. Toutes les séquences de touches du clavier KVM, excepté PrtSc, sont envoyées au serveur, avec la souris KVM. Appuyez sur la touche **Impr écran** pour quitter la console du serveur et revenir au menu KVM.


Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 5:
Media State . . . . . : Media disconnected
C:\Documents and Settings\Administrator>

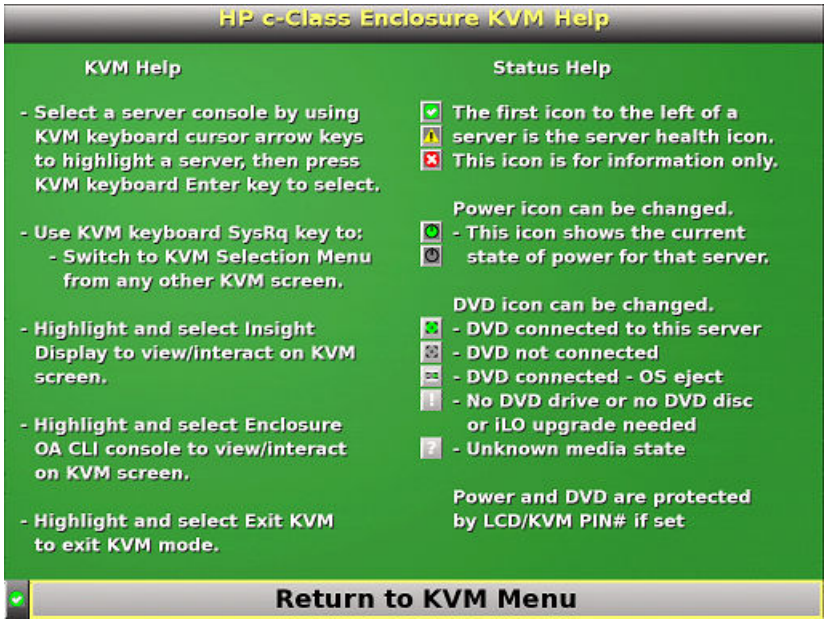
REMARQUE : Pour les résolutions de 1 024 x 768 à 1 600 x 1 200, la résolution d'écran correspond à la résolution de l'écran de la console du serveur. Les résolutions de console de serveur inférieures à 1 024 x 768 entraînent un affichage sur une partie de l'écran KVM Onboard Administrator en mode 1 024 x 768. Pour les résolutions de console de serveur supérieures à 1 600 x 1 200, un message d'avertissement s'affiche et vous revenez à l'écran Enclosure KVM Menu.

- Server Power (Alimentation du serveur) : sélectionnez cette icône d'alimentation de serveur pour modifier l'état d'alimentation du serveur.
- Server DVD (DVD de serveur) : sélectionnez cette icône de DVD de serveur pour modifier la connexion de DVD de boîtier pour ce serveur.
- Server Health (Intégrité de serveur) : sélectionnez cette icône d'intégrité pour afficher l'état d'intégrité actuel de ce serveur.
- Insight Display : sélectionnez le bouton Insight Display pour accéder aux écrans Insight Display du menu KVM.

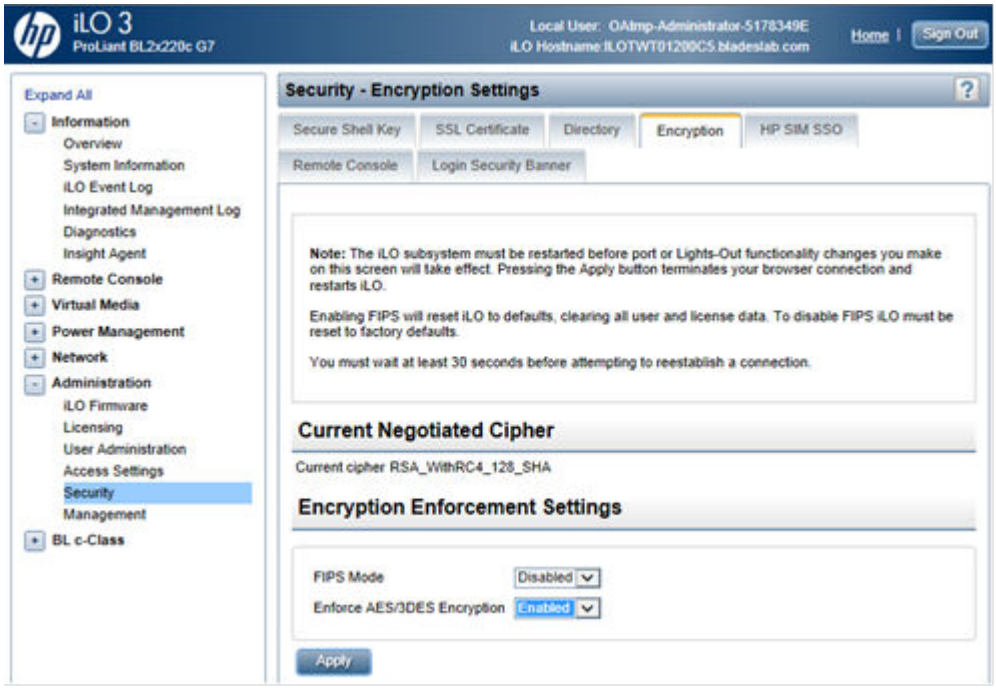
- OA CLI (Interface CLI OA) : sélectionnez **OA CLI** pour lancer l'interface CLI du module Onboard Administrator. Connectez-vous au module Onboard Administrator à l'aide du clavier KVM. Cette opération lance une console plein écran vers l'interface de ligne de commande du module Onboard Administrator actif. Pour quitter la console de l'interface CLI du module Onboard Administrator et revenir au menu KVM, appuyez sur la touche **Impr écran**.


HP BladeSystem Onboard Administrator
(C) Copyright 2006-2008 Hewlett-Packard Development Company, L.P.
Type 'HELP' to display a list of valid commands.
Type 'HELP <command>' to display detailed information about a specific command.
Type 'HELP HELP' to display more detailed information about the help system.
OA-002264343171> show oa network
Onboard Administrator #2 Network Information:
Name: OA-002264343171
DHCP: Enabled - Dynamic DNS
IP Address: 16.84.189.156
Netmask: 255.255.252.0
Gateway Address: 16.84.188.1
Primary DNS: 16.110.135.51
Secondary DNS: 16.110.135.52
MAC Address: 00:22:64:34:31:71
Link Settings: Auto-Negotiation, 100 Mbit, Full Duplex
Link Status: Active
Enclosure IP Mode: Disabled
OA-002264343171> _

- Help (Aide) : sélectionnez **Help** pour afficher des informations d'aide KVM.


HP c-Class Enclosure KVM Help
KVM Help
- Select a server console by using KVM keyboard cursor arrow keys to highlight a server, then press KVM keyboard Enter key to select.
- Use KVM keyboard SysRq key to:
- Switch to KVM Selection Menu from any other KVM screen.
- Highlight and select Insight Display to view/interact on KVM screen.
- Highlight and select Enclosure OA CLI console to view/interact on KVM screen.
- Highlight and select Exit KVM to exit KVM mode.
Status Help
The first icon to the left of a server is the server health icon.
This icon is for information only.
Power icon can be changed.
- This icon shows the current state of power for that server.
DVD icon can be changed.
- DVD connected to this server
- DVD not connected
- DVD connected - OS eject
- No DVD drive or no DVD disc or iLO upgrade needed
- Unknown media state
Power and DVD are protected by LCD/KVM PIN# if set
Return to KVM Menu

REMARQUE : Lorsque le module Onboard Administrator est en mode FIPS, le paramètre d'accès à la sécurité iLO, Enforce AES/3DES Encryption, doit être activé. Pour changer le paramètre iLO, naviguez vers **Administration>Security>Encryption** (Administration>Sécurité>Chiffrement). La connexion KVM à iLO2 n'est pas prise en charge en mode FIPS ON/DEBUG.



5 Assistant First Time Setup

Avant de commencer

Avant d'exécuter l'assistant First Time Setup (Assistant de première installation), effectuez les opérations suivantes :

1. Installez les modules Onboard Administrator.
2. Connectez les modules Onboard Administrator au réseau.
3. Finalisez l'installation à l'aide de l'assistant d'installation Insight Display. Configurez au moins l'adresse IP du module Onboard Administrator actif.
4. Exécutez l'installation de l'écran Insight Display.

Connexion au module Onboard Administrator

1. Ouvrez un navigateur et connectez-vous au module HP BladeSystem Onboard Administrator actif à l'aide de l'adresse IP qui a été configurée lors de l'exécution de l'assistant d'installation de l'écran Insight Display.
2. Entrez le nom d'utilisateur et le mot de passe d'administration initial de votre compte HP BladeSystem Onboard Administrator, indiqués sur l'étiquette fixée au module Onboard Administrator.

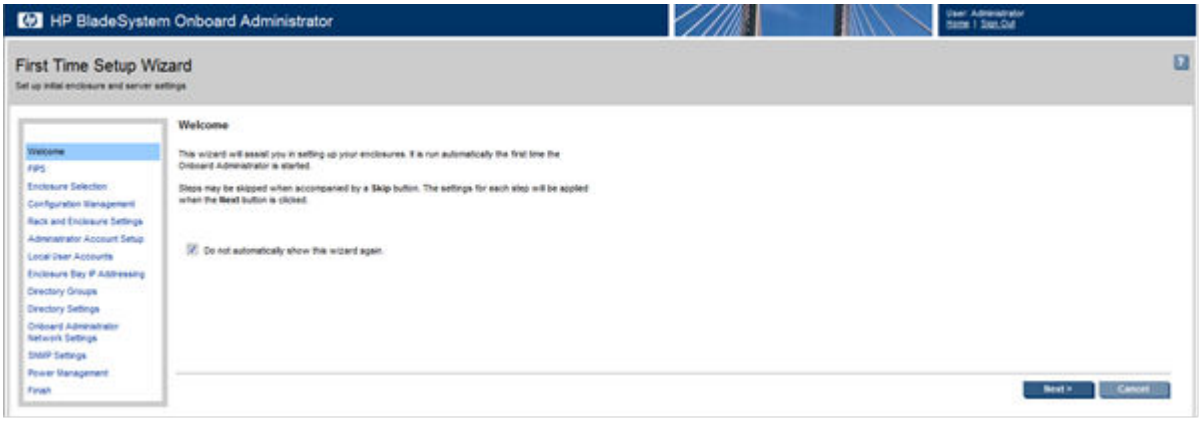
Problèmes possibles qui peuvent se produire lors de la connexion :

- Vous ne saisissez pas les informations correctement. Les mots de passe font la distinction entre les majuscules et les minuscules.
- Les informations du compte que vous saisissez n'ont pas été configurées pour HP BladeSystem Onboard Administrator.
- Le nom d'utilisateur que vous saisissez a été supprimé, désactivé ou verrouillé.
- Le mot de passe de ce compte doit être modifié.
- Vous tentez de vous connecter à partir d'une adresse IP qui n'est pas correcte pour le compte spécifié.
- Si les problèmes de connexion persistent, contactez votre administrateur.

Le module Onboard Administrator exécute automatiquement l'assistant First Time Setup lors de votre première connexion.

Pour naviguer dans l'assistant d'installation, cliquez sur **Next** (Suivant) pour enregistrer vos modifications et passer à l'étape suivante. Cliquez sur **Skip** (Ignorer) si vous souhaitez quitter l'étape sans enregistrer les modifications.

Vous pouvez revenir aux étapes précédentes de l'assistant en les sélectionnant dans l'arborescence à gauche. Vous pouvez également exécuter à nouveau l'assistant à tout moment en le sélectionnant dans le menu Wizards (Assistants).



Préférences de l'utilisateur

Pour modifier la langue d'affichage, sélectionnez une langue d'affichage dans la liste, puis cliquez sur **Apply** (Appliquer). La langue sélectionnée remplace le paramètre actuel de préférence de langue du navigateur et est conservée avec les sessions d'interface utilisateur ultérieures avec le même module Onboard Administrator. Toutefois, le paramètre ne s'applique pas pour les sessions d'interface utilisateur avec d'autres modules Onboard Administrator. (Le paramètre repose sur un cookie qui est valide uniquement pour l'adresse IP du module Onboard Administrator actuel. Si vous modifiez l'adresse IP, le paramètre doit être appliqué à nouveau à partir de la nouvelle adresse.)

Si vous souhaitez afficher la langue pour les connexions à d'autres interfaces utilisateur de module Onboard Administrator à l'aide de ce navigateur :

1. Ajoutez la langue en haut de la liste de langues préférées du navigateur.
2. Sur l'écran de préférences de l'utilisateur Onboard Administrator, sélectionnez « Use browser settings » (Utiliser paramètres de navigateur) dans la liste déroulante.
3. Actualisez la langue d'affichage en cliquant sur **Apply** (Appliquer). Le pack de langues correspondant doit être installé sur les autres modules Onboard Administrator. Pour plus d'informations sur l'installation d'un pack de langues, consultez l'onglet Active Onboard Administrator Language Pack.

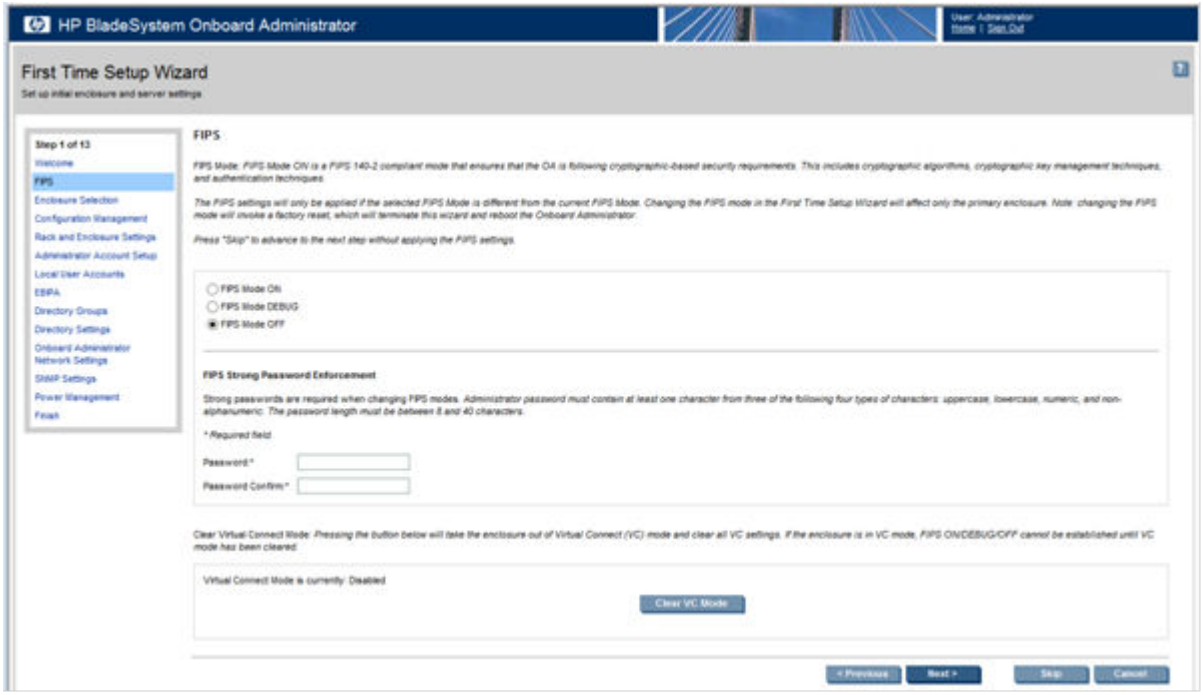
   Si le paramètre « Use browser settings » est déjà défini, actualisez la langue d'affichage sans modifier le paramètre en cliquant sur **Refresh** (Actualiser).

La liste déroulante de préférences utilisateur inclut uniquement les langues qui ont été installées ou qui sont intégrées au module Onboard Administrator. Si vous définissez la préférence de langue de navigateur sur une langue qui n'est pas répertoriée, l'interface Onboard Administrator n'utilise pas le paramètre de langue de navigateur ; l'interface utilisateur utilise la langue par défaut (en anglais) à la place.

REMARQUE : Si le chargement de la langue d'affichage ne s'effectue pas correctement, effacez le cache du navigateur et actualisez l'application en actualisant ou rechargeant le navigateur.

REMARQUE : Si vous utilisez un pack de langues installé avec l'interface Onboard Administrator et que le navigateur n'affiche pas tous les caractères correctement, assurez-vous que le système d'exploitation dispose de la prise en charge installée de la langue correspondante.

FIPS



Mode FIPS

REMARQUE : La modification du mode FIPS sur ON/DEBUG ou OFF ne prend pas effet sauf si le mode VC est désactivé.

REMARQUE : Lorsque le module Onboard Administrator fonctionne en mode FIPS, la longueur minimale de la clé RSA ne doit pas être inférieure à 2 048 bits, et l'algorithme de hachage de la signature doit être SHA1, SHA-224, SHA-256, SHA-384 ou SHA-512.

- **FIPS Mode OFF** : active l'utilisation d'algorithmes non approuvés par FIPS 140-2.
- **FIPS Mode ON** : met en œuvre l'utilisation du module Onboard Administrator dans un mode approuvé par FIPS 140-2. Ce paramètre prend en charge l'utilisation de chiffrements et de protocoles cryptographiques approuvés.
- **FIPS Mode DEBUG** : définit le module Onboard Administrator sur un environnement similaire au mode FIPS ON, mais avec l'option de prise en charge de débogage par HP. Le mode FIPS DEBUG possède les fonctionnalités du mode FIPS ON, mais il n'est pas considéré comme compatible FIPS en raison de l'option de débogage.

Le module Onboard Administrator redémarre une fois que toutes les modifications ont été apportées.

REMARQUE : Tous les paramètres existants sont perdus lorsque vous exécutez cette opération. Toutes les modifications apportées au paramètre du mode FIPS effectuent une opération de restauration sur les paramètres usine par défaut.

REMARQUE : Si le mode FIPS est sur ON/DEBUG, assurez-vous qu'un mot de passe robuste est défini.

Icônes d'état du mode FIPS

En mode FIPS ON ou DEBUG activé, l'état actuel du mode FIPS est indiqué par une icône affichée sur la barre d'en-tête du module Onboard Administrator sur les écrans de l'interface graphique. Il est également affiché sur la page de connexion du module Onboard Administrator dans la colonne Connection de la table de boîtiers. Les icônes d'état sont décrites dans le tableau suivant :

Icône du mode FIPS	Description
	Le mode FIPS est activé (ON).
	Le mode FIPS ON a un ou plusieurs avertissements. Pour déterminer la nature de l'avertissement, placez le pointeur de la souris sur l'icône.
	Le mode FIPS DEBUG est activé.
	Le mode FIPS DEBUG a un ou plusieurs avertissements. Pour déterminer la nature de l'avertissement, placez le pointeur de la souris sur l'icône.

Exécution du mot de passe robuste FIPS

En cas de basculement entre des modes FIPS disponibles, les mots de passe robustes sont activés, la longueur minimum du mot de passe est définie sur huit caractères et un nouveau mot de passe de compte Administrateur est demandé. En outre, en cas de basculement sur le mode FIPS ON ou le mode FIPS DEBUG, le mode IP de boîtier et les protocoles Telnet, SNMPv1 et SNMPv2 sont désactivés alors que SNMPv3 est disponible.

Pour enregistrer les paramètres, cliquez sur **Next** (Suivant). En cas de boîtiers liés, seul le boîtier principal est concerné. Pour passer à l'étape suivante sans appliquer les paramètres FIPS, cliquez sur **Skip** (Ignorer).

REMARQUE : L'entrée et la sortie du mode FIPS effectuent une opération de restauration usine et verrouillent le panneau Insight Display (LCD). Si le module Onboard Administrator a été précédemment configuré avec une adresse IP statique, il prend par défaut une adresse DHCP jusqu'à ce qu'il soit reconfiguré avec une adresse IP statique. La récupération nécessite l'accès à la console série du module Onboard Administrator pour exécuter la commande `SHOW OA NETWORK` pour détecter la nouvelle adresse IP du module Onboard Administrator.

Le terme Mode FIPS est utilisé dans ce document et dans le produit pour décrire la fonction, et non son état de validation. Le processus de validation FIPS est long, c'est pourquoi toutes les versions sont validées FIPS. Pour plus d'informations sur l'état FIPS actuel de cette version ou de toute autre version du microprogramme, reportez-vous aux documents suivants :

- Programme de validation des modules cryptographiques FIPS 140-1 et FIPS 140-2 de la liste de processus (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf)
- Liste des fournisseurs FIPS 140-1 et FIPS 140-2 (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm)

Effacement du mode VC

L'effacement du mode VC supprime tous les paramètres VC du boîtier. Mettez hors tension tous les serveurs configurés VC avant d'effacer le mode VC. Si les serveurs ne sont pas mis hors tension, ils risquent de conserver leurs paramètres VC jusqu'à leur redémarrage. Vous devez effacer le mode VC avant de passer au mode FIPS OFF/ON/DEBUG.

Pour effacer le mode VC :

1. Cliquez sur **Clear VC Mode** (Effacer mode VC). Un écran de confirmation s'affiche, indiquant un message signifiant `Tous les serveurs doivent être mis hors tension et non configurés par Virtual Connect avant l'effacement du mode VC. Souhaitez-vous vraiment effacer le mode VC ?`
2. Cliquez sur **OK**.

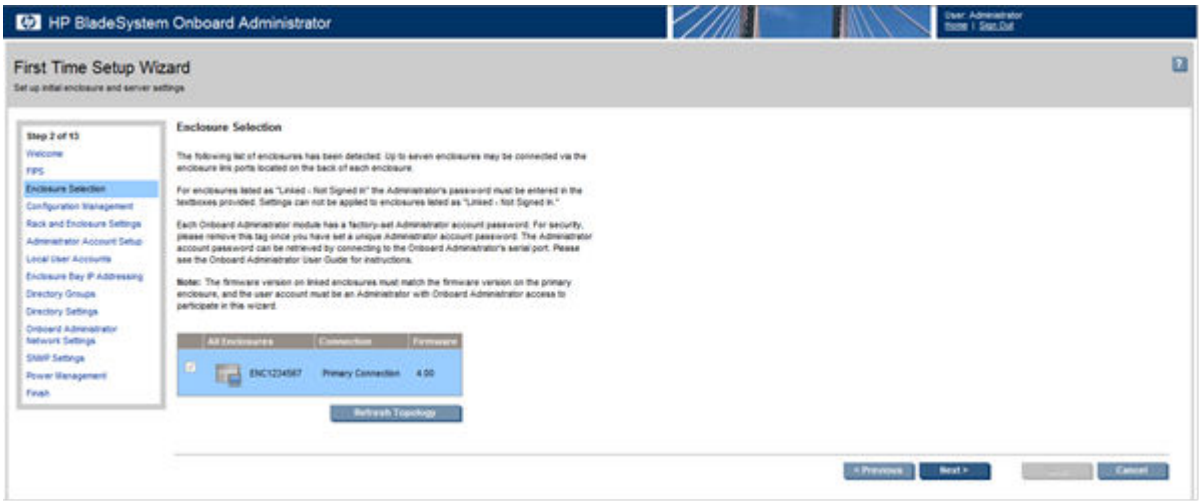
Paramètres de sécurité avancés

Vous pouvez activer ou désactiver les protocoles de sécurité et les chiffrements sélectionnés à partir de l'onglet **Enclosure Settings>Network Access>FIPS** (Onglet FIPS à la page 139) (Onglet FIPS à la page 139).

Écran Enclosure Selection

L'écran Enclosure Selection (Sélection de boîtier) affiche tous les boîtiers détectés et sélectionne le boîtier actif, le boîtier auquel vous êtes connecté par défaut. La case à cocher en regard de chaque boîtier permet de sélectionner ou de désélectionner le boîtier correspondant. Pour cocher la case de tous les boîtiers, sélectionnez la case à cocher **All Enclosures** (Tous les boîtiers).

Pour actualiser les informations de topologie du rack, cliquez sur **Refresh Topology** (Actualiser la topologie). Lorsque l'option **Refresh Topology** est sélectionnée, l'écran Enclosure Selection bascule sur le mode lié et tous les boîtiers liés apparaissent.



Les boîtiers liés sont dans l'un des états suivants :

- Linked - Not Signed In (Lié, non connecté). Sélectionnez le boîtier et entrez le mot de passe Administrateur dans la zone de texte de mot de passe. Pour authentifier le boîtier, cliquez sur **Next** (Suivant).
- Linked - Not Signed In (Lié, non connecté) avec une icône de lecteur de carte. Cet état indique que le boîtier lié dispose de l'authentification à deux facteurs activée mais n'est pas authentifié. Cet état se produit sous deux conditions :
  - Si la configuration n'est pas prise en charge. Le boîtier principal doit être activé pour l'authentification à deux facteurs et les deux boîtiers (principal et lié) doivent avoir les mêmes informations d'identification pour que le boîtier lié puisse s'authentifier via l'authentification à deux facteurs. Si le boîtier principal ne dispose pas de l'authentification à

deux facteurs activée, vous ne pouvez pas sélectionner le boîtier lié avec l'authentification à deux facteurs activée.

- Si vous cliquez sur le lien Sign Out (Déconnexion) sur un boîtier doté de l'authentification à deux facteurs activée qui est déjà authentifié, cet état s'affiche. Si vous sélectionnez ce boîtier, une authentification est tentée lorsque vous cliquez sur **Next** (Suivant).

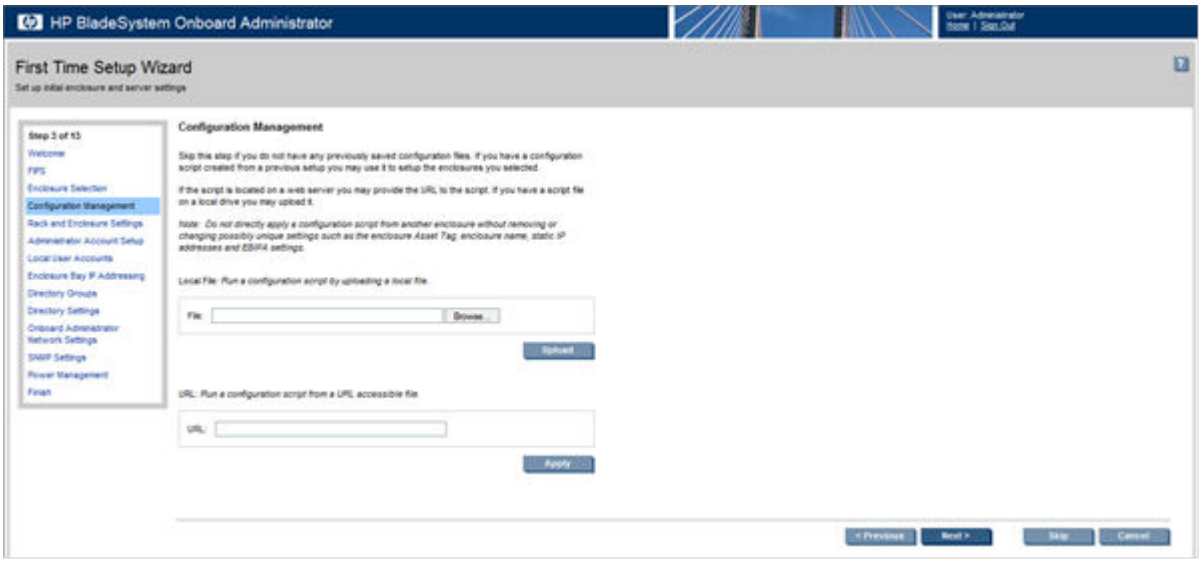
- Lié, connecté avec ou sans icône de lecteur de carte. Cet état indique que le boîtier lié est authentifié. Si les informations du boîtier ne sont pas déjà chargées, elles le sont lorsque vous cliquez sur **Next** (Suivant).

Si plusieurs boîtiers sont répertoriés dans l'écran Enclosure Selection, sélectionnez celui à installer, puis cliquez sur **Next** (Suivant).

Pour connaître les valeurs possibles et la description de chaque champ, consultez la section « Écran Enclosure Information » (Écran Enclosure Information à la page 113).

Écran Configuration Management

L'écran Configuration Management (Gestion de la configuration) permet d'installer les boîtiers sélectionnés à partir d'un fichier de configuration enregistré lors d'une précédente installation. Vous pouvez exécuter des scripts pour plusieurs modules Onboard Administrator avant de quitter l'écran courant.



Pour installer les boîtiers sélectionnés à l'aide d'un fichier de configuration :

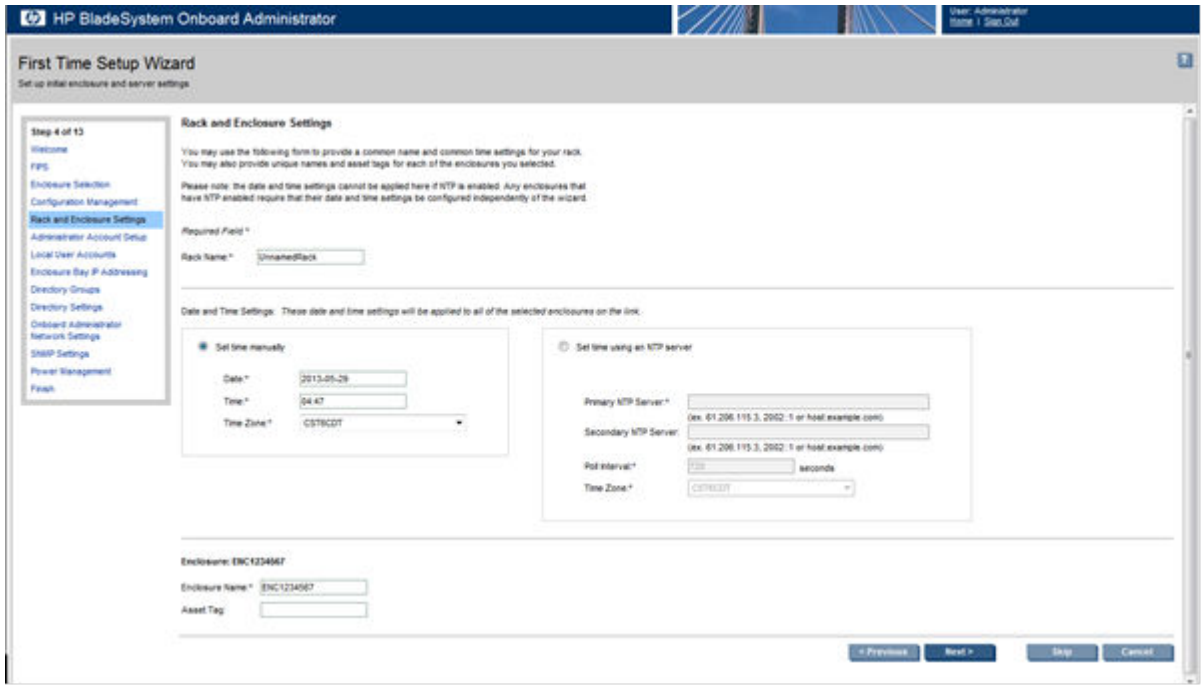
Sélectionnez le boîtier vers lequel charger le fichier de configuration. Vous pouvez uniquement charger le fichier de configuration vers un boîtier, même si vous avez sélectionné **All Enclosures** (Tous les boîtiers) sur l'écran **Enclosure Selection**. Vous pouvez sélectionner un fichier local, une URL ou un fichier USB :

- **Fichier local** : vous pouvez rechercher le fichier de configuration ou vous pouvez entrer son chemin d'accès dans la zone de texte. Le nombre maximum de caractères dans le chemin du fichier est 256. Saisissez le chemin du fichier de configuration, cliquez sur **Upload** (Charger).
- **URL** : saisissez un chemin de type http:// pour le fichier de configuration si ce dernier est stocké sur un serveur Web. Le nombre maximum de caractères dans le chemin du fichier est 256. Après avoir saisi l'URL, cliquez sur **Apply** (Appliquer).
- **Fichier USB** : vous pouvez sélectionner un fichier de configuration sur une clé USB branchée sur le boîtier. Sélectionnez le fichier de configuration approprié à partir de la liste déroulante. Une fois le fichier de configuration sélectionné, cliquez sur **Apply** (Appliquer). Cette option apparaît uniquement si une clé USB est branchée sur le boîtier.

Une fois l'emplacement du fichier sélectionné, une boîte de dialogue affiche les résultats.

Écran Rack and Enclosure Settings

Utilisez ce formulaire pour fournir les paramètres de nom courant et d'heure de votre rack et attribuer des noms uniques et des étiquettes à vos boîtiers.



Champ	Valeur possible	Description
Rack Name (Nom du rack)	De 1 à 32 caractères, notamment tous les caractères alphanumériques, le tiret (-) et le trait de soulignement (_).	Nom du rack sur lequel le boîtier est installé.
Date and Time Settings (Paramètres de date et heure)	• Définir l'heure manuellement • Définir l'heure à l'aide d'un serveur NTP	La méthode utilisée pour attribuer la date et l'heure à tous les boîtiers sélectionnés sur la liaison
Date	aaaa-mm-jj, où : • mm est un entier compris entre 1 et 12	Date courante attribuée au boîtier.

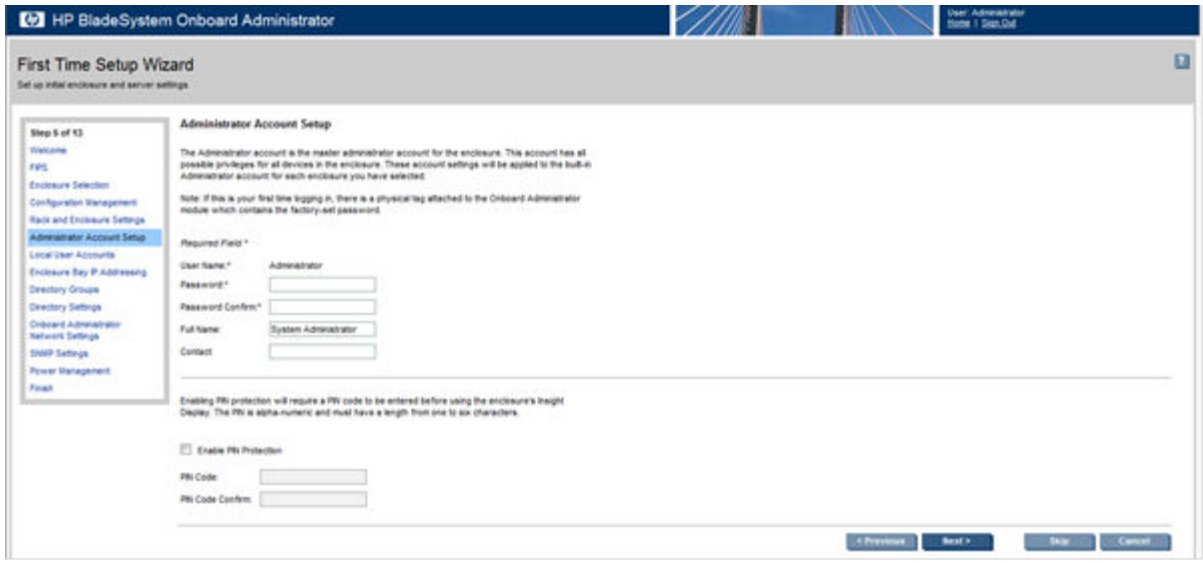
Champ	Valeur possible	Description
	• jj est un entier compris entre 1 et 31	
Time (Heure)	hh:mm (format 24 heures) • hh est un entier compris entre 0 et 23 • mm est un entier compris entre 0 et 59	Heure courante attribuée au boîtier.
Time Zone (Fuseau horaire)	Paramètres des fuseaux horaires • Paramètres de fuseaux horaires de la zone Afrique (Paramètres de fuseaux horaires de la zone Afrique à la page 433) • Paramètres de fuseaux horaires de la zone Amérique (Paramètres de fuseaux horaires de la zone Amérique à la page 434) • Paramètres de fuseaux horaires de la zone Asie (Paramètres de fuseaux horaires de la zone Asie à la page 436) • Paramètres de fuseaux horaires universels (Paramètres de fuseaux horaires universels à la page 433) • Paramètres des fuseaux horaires des zones océaniques (Paramètres de fuseaux horaires de la zone Océanie à la page 437) • Paramètres de fuseaux horaires de la zone Europe (Paramètres de fuseaux horaires de la zone Europe à la page 438) • Paramètres de fuseaux horaires de la zone polaire (Paramètres de fuseaux horaires de la zone polaire à la page 438)	Fuseau horaire attribué au boîtier
Primary NTP Server (Serveur NTP principal)	• Adresse IPv4 : ###.###.###.### où ### est compris entre 0 et 255. • Adresse Ipv6 : ####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. • Nom DNS : peut comprendre entre 1 et 64 caractères notamment tous les caractères alphanumériques et le tiret (-).	Adresse IP ou nom DNS du serveur NTP principal qui fournit les informations de date et heure
Secondary NTP Server (Serveur NTP secondaire)	• Adresse IPv4 : ###.###.###.### où ### est compris entre 0 et 255.	Adresse IP ou nom DNS du serveur NTP secondaire qui fournit les informations de date et heure

Champ	Valeur possible	Description
	• Adresse Ipv6 : ####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. • Nom DNS : peut comprendre entre 1 et 64 caractères notamment tous les caractères alphanumériques et le tiret (-).	
Poll Interval (Intervalle d'interrogation)	Entier compris entre 60 et 86400	Intervalle de scrutation en secondes du serveur NTP
Enclosure name (Nom du boîtier)	De 1 à 32 caractères, notamment tous les caractères alphanumériques, le tiret (-) et le trait de soulignement (_).	Nom du boîtier sélectionné.
Asset Tag (Étiquette d'inventaire)	De 0 à 32 caractères, notamment tous les caractères alphanumériques, le tiret (-) et le trait de soulignement (_).	L'étiquette d'inventaire est utilisée à des fins de contrôle des stocks. L'étiquette par défaut est vierge.

Pour plus d'informations sur la connexion de boîtiers, reportez-vous au *Manuel de l'utilisateur du boîtier HP BladeSystem c7000*.

Écran Administrator Account Setup

L'écran Administrator Account Setup (Configuration du compte administrateur) affiche au départ le nom du boîtier actif et les paramètres courants. Si plusieurs boîtiers ont été sélectionnés sur l'écran Enclosure Selection, un bouton est activé pour permettre d'afficher les entrées distinctes de chaque module Onboard Administrator sélectionné.



Champ	Valeur possible	Description
Full Name (Nom complet)	De 0 à 20 caractères, notamment tous les caractères alphanumériques, le tiret (-), le trait de soulignement (_) et l'espace.	Nom complet de l'utilisateur
Contact	De 0 à 20 caractères, notamment tous les caractères alphanumériques, le tiret (-), le trait de soulignement (_) et l'espace.	Informations de contact pour le compte utilisateur. Les informations de contact peuvent être le nom d'une personne, un numéro de téléphone ou toute autre information utile.
Administrator Password (Mot de passe administrateur)	De 3 à 40 caractères, notamment tous les caractères imprimables.	Mot de passe du compte utilisateur.
Administrator Password Confirm (Confirmation du mot de passe administrateur)	De 3 à 40 caractères, notamment tous les caractères imprimables.	Doit correspondre à la valeur du mot de passe administrateur.
Enable Insight Display PIN protection (Activer la protection du code PIN de l'écran Insight Display)	Activez ou désactivez la case à cocher	Cochez cette case pour demander de saisir un code PIN pour accéder à l'écran Insight Display du boîtier.
Pin Code (Code PIN)	De 1 à 6 caractères, à partir des jeux de caractères de 0 à 9, a à z et A à Z.	Code PIN de l'Insight Display du boîtier.
PIN Code Confirm (Confirmation du numéro d'identification personnelle)	De 1 à 6 caractères, à partir des jeux de caractères de 0 à 9, a à z et A à Z.	Doit correspondre à la valeur du code PIN de l'écran Insight Display.

REMARQUE : Lorsque le module Onboard Administrator fonctionne en mode FIPS ON/DEBUG, la protection par code PIN ne peut pas être désactivée.

Écran Local User Accounts

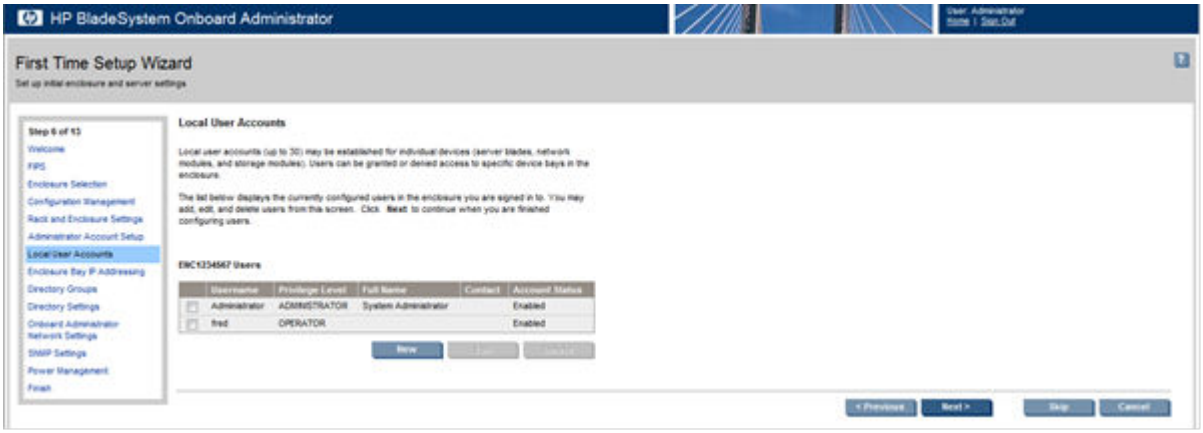
L'écran Local User Accounts (Comptes utilisateurs locaux) affiche les comptes utilisateur attribués au module Onboard Administrator actif et offre la possibilité d'ajouter, de modifier et de supprimer des comptes.

New (Nouveau) : pour ajouter un nouvel utilisateur au boîtier sélectionné, cliquez sur le bouton **New**. L'écran Add Local User (Ajout d'utilisateur local) s'affiche.

REMARQUE : 30 comptes utilisateur au maximum peuvent être configurés en mode FIPS OFF, alors que 21 comptes utilisateur au maximum peuvent être configurés en mode FIPS ON ou DEBUG. La limite du nombre d'utilisateurs maximum inclut des comptes réservés tels que les comptes administrateur et Virtual Connect.

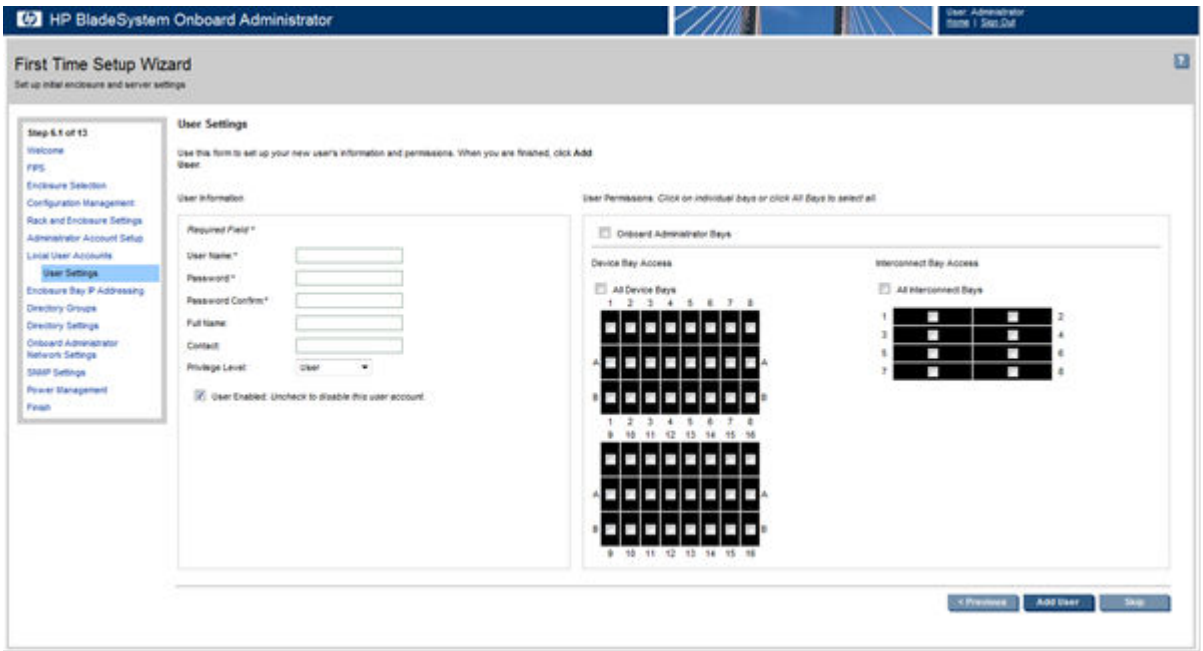
Edit (Modifier) : sélectionnez un utilisateur (vous ne pouvez en sélectionner qu'un seul) en cochant la case située en regard du nom de l'utilisateur. Pour modifier les paramètres de l'écran Edit Local User (Modification d'utilisateur local), cliquez sur **Edit** (Modifier).

Delete (Supprimer) : sélectionnez un ou plusieurs utilisateurs à supprimer en cochant la case en regard du nom de chaque utilisateur. Pour supprimer les comptes, cliquez sur **Delete**. Si vous essayez de supprimer le dernier compte administrateur restant, un avertissement d'alerte indique qu'un compte administrateur doit exister et l'action de suppression est annulée.



Écran User Settings

L'écran User Settings (Paramètres utilisateur) affiche les informations utilisateur pouvant être configurées. Entrez les informations utilisateur dans les sections User Information (Informations utilisateur) et User Permissions (Autorisations utilisateur). Pour enregistrer les informations, cliquez sur **Add User** (Ajouter utilisateur). Pour revenir à l'écran Local User Accounts, cliquez sur **Cancel** (Annuler).



Pour chaque utilisateur ajouté, cochez les cases appropriées pour leur accorder l'accès aux baies de serveur et d'interconnexion.

Pour connaître les valeurs possibles et la description de chaque champ, consultez la section « Ajout d'un utilisateur local » (Ajout d'un utilisateur local à la page 329).

Adressage IP des baies de boîtiers

Les écrans Enclosure Bay IP Addressing (Adressage IP des baies de boîtiers) de l'assistant First Time Setup permettent de configurer des adresses IPv4 et IPv6 fixes pour les baies de boîtiers Onboard Administrator. La fonctionnalité EBIPA du module Onboard Administrator aide à configurer une adresse IP fixe basée sur le numéro de baie, qui conserve l'adresse IP d'une baie particulière, même si un périphérique est remplacé à chaud. L'interface de gestion des composants branchés sur

les baies doit être définie pour le type DHCP. EBIPA ne peut être utilisé que si les périphériques sont configurés pour démarrer à partir de DHCP. Si un périphérique est configuré pour une adresse IP statique, il doit être reconfiguré manuellement pour DHCP afin de basculer sur l'adresse IP EBIPA.

REMARQUE : La documentation du module Onboard Administrator se réfère à des adresses IP EBIPA telles que des « adresses IP fixes » ou des « adresses DHCP fixes », ce qui signifie que chacune de ces adresses correspond à une adresse IP associée de façon permanente à un certain nombre de baies spécifiques indépendantes du dispositif actuel fixé à la baie.

Les baies iLO de lame de serveur et les baies de gestion de module d'interconnexion peuvent obtenir des adresses IP sur le réseau de gestion de différentes manières : adressage IP dynamique à l'aide d'un serveur DHCP externe, adressage IP statique, SLAAC via annonces de routeur (IPv6 uniquement) ou EBIPA. Si votre réseau dispose d'un service DHCP ou si vous souhaitez affecter manuellement des adresses IP statiques l'une après l'autre aux lames de serveur et aux modules d'interconnexion, cliquez sur **Skip** (Ignorer) pour contourner la configuration de l'adressage IP des baies de boîtiers.

L'adressage EBIPA attribue uniquement des adresses IP DHCP fixes à l'interface de gestion pour des modules d'interconnexion et systèmes iLO de serveur sur le réseau de gestion interne au boîtier. L'adressage EBIPA ne permet pas d'attribuer des adresses IP à d'autres périphériques sur le réseau de gestion externe au boîtier et ne peut pas être utilisé comme serveur DHCP sur le réseau de données.

La lame de serveur de iLO choisit l'adressage DHCP par défaut, obtenu via le connecteur réseau de Onboard Administrator intégré en cours. Les modules d'interconnexion disposant d'une connexion réseau de supervision à Onboard Administrator peuvent également choisir l'adresse DHCP par défaut.

REMARQUE : EBIPA applique des adresses IP uniques pour toutes les baies, même si les baies se trouvent sur un autre VLAN.

Instructions de configuration EBIPA

Cette section fournit des informations de configuration générales. Pour obtenir des informations de configuration spécifiques à IPv4 ou IPv6, consultez les sections correspondantes qui suivent.

Si votre installation préfère l'attribution d'adresses IP fixes, vous pouvez spécifier des adresses fixes uniques individuellement pour chacune des baies iLO de lame de serveur et des baies de gestion du module d'interconnexion, ou vous pouvez utiliser EBIPA pour attribuer une plage d'adresses IP fixes à chaque baie de lame de serveur et de module d'interconnexion. Si vous spécifiez des adresses fixes individuellement, le masque de sous-réseau (IPv4), la passerelle, les serveurs DNS, les serveurs NTP (interconnexion IPv4) et le nom de domaine peuvent être identiques ou différents pour chaque baie. Si vous utilisez EBIPA pour attribuer une plage d'adresses fixes, vous devez spécifier la première adresse IP dans la plage et le masque de sous-réseau. Lorsque vous cliquez sur le bouton fléché vers le bas **Autofill** (Remplissage auto) de cette baie, les baies énumérées en dessous de cette dernière sont automatiquement attribuées à des adresses IP consécutives. Le masque de sous réseau, la passerelle, les serveurs DNS, les serveurs NTP et le nom de domaine sont également copiés dans chacune des baies consécutives de la liste.

Par exemple, si vous spécifiez l'adresse IPv4 16.100.226.21 pour la baie EBIPA 1 et que vous utilisez la fonctionnalité Autofill, les baies 1 à 16 sont affectées à des adresses IP consécutives dans la plage comprise entre 16.100.226.21 et 16.100.226.36. Si vous spécifiez 16.200.139.51 pour la baie d'interconnexion 3 et que vous utilisez cette fonctionnalité, les baies d'interconnexion 3 à 8 sont affectées à des adresses IP consécutives dans la plage comprise entre 16.200.139.51 et 16.200.139.56.

REMARQUE : Le bouton **Autofill** (Remplissage auto) ne remplit que tous les champs d'adresse si le champ d'adresse associé à la première adresse de la liste est sélectionné. Par exemple, le remplissage automatique de l'adresse 1 remplira les adresses 1 à 16, le remplissage automatique de l'adresse 2 remplira les adresses 2 à 16, etc.

Lors de l'utilisation du remplissage automatique, spécifiez un masque de sous-réseau IPv4 ou un préfixe de sous-réseau IPv6 qui autorise suffisamment d'adresses disponibles sur le sous-réseau associé pour remplir tous les champs d'adresse correspondant au nombre total de baies sélectionnées. Si vous spécifiez un préfixe ou un masque de sous-réseau qui ne répond pas à cette exigence, « Invalid IP Address » (Adresse IP non valide) s'affiche dans le champ d'adresse de chaque baie pour laquelle une adresse ne peut pas être générée.

Si vous utilisez des adresses IP statiques pour les processeurs de supervision, la commande `hponcfg` du module Onboard Administrator peut être utilisée pour envoyer le script RIBCL des paramètres réseau iLO à un module iLO si ce module a déjà une adresse IP. EBIPA peut être utilisé pour démarrer les adresses IP des iLO, afin que la commande `hponcfg` du module Onboard Administrator puisse être utilisée pour envoyer des scripts de configuration à ces iLO. Les modifications apportées aux paramètres de réseau iLO entraînent la réinitialisation par le système iLO de son réseau et l'interruption de toute connexion actuelle pendant quelques secondes.

Si vous possédez des lames de serveur double densité, ne configurez pas les paramètres EBIPA pour les baies de base (baie 1, 2, et ainsi de suite). Configurez les baies de côté A (1A, 2A, et ainsi de suite) et les baies de côté B (1B, 2B, et ainsi de suite). L'utilisation de la fonctionnalité Autofill attribue des adresses IP consécutives aux baies répertoriées sous la baie où vous indiquez la première adresse IP de la plage (par exemple, si vous spécifiez l'adresse IP de la baie 1A et que vous utilisez la fonctionnalité Autofill, les baies 2A, 3A, et ainsi de suite sont affectées à des adresses consécutives).

Pour configurer les baies d'interconnexion, utilisez la liste d'interconnexion (située en dessous de la liste des périphériques, sur le même écran de l'assistant).

Pour appliquer les paramètres, cliquez sur **Next** (Suivant).

Les serveurs dans les baies de périphérique vont obtenir automatiquement les adresses EBIPA de baies de périphérique en quelques minutes, mais les modules commutateurs d'interconnexion doivent être redémarrés manuellement en cliquant sur le bouton **Virtual Power** (Alimentation virtuelle) dans chaque page d'informations du module d'interconnexion Onboard Administrator.

Configuration de votre boîtier à l'aide de EBIPA sans connexion réseau active

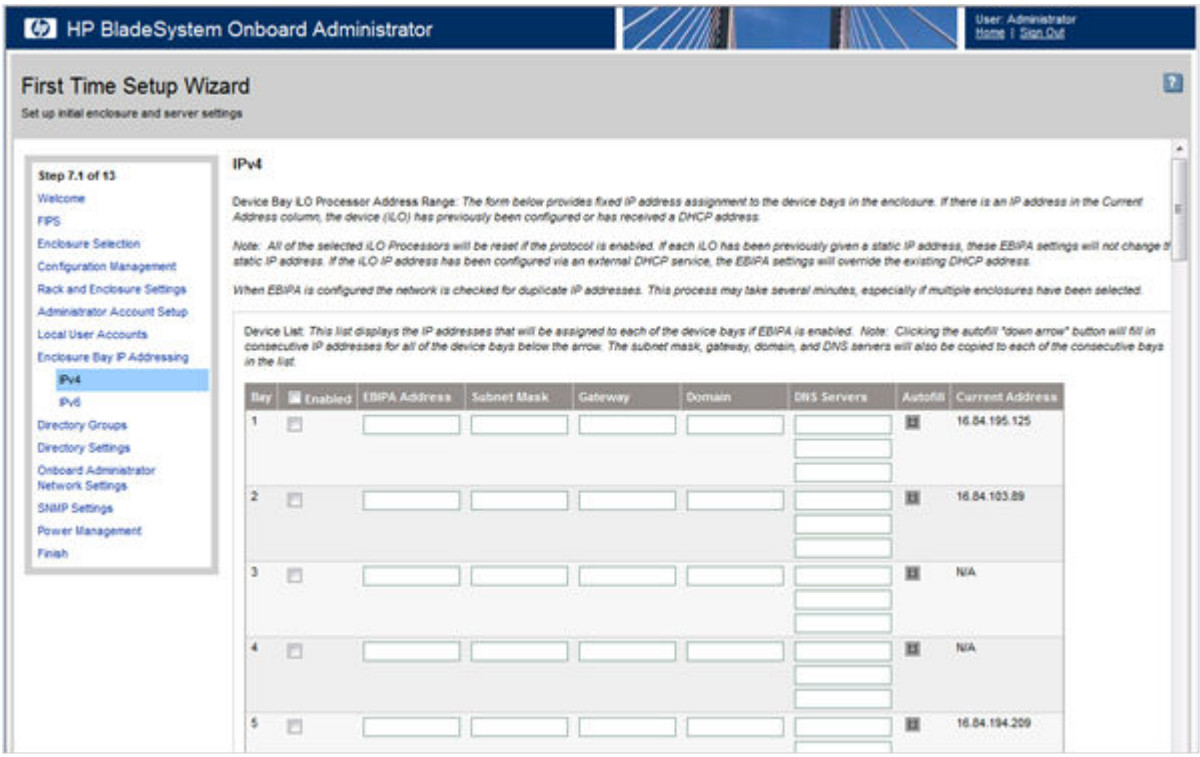
1. Configurez une adresse IP statique pour chaque module Onboard Administrator utilisant Insight Display et notez l'adresse IP de service OA actif sur l'écran Info du boîtier Insight Display. Reliez le PC client au port de service du boîtier (connecteur « bas » de liaison de boîtier) entre les baies OA avec un cordon de raccordement Ethernet standard. La carte réseau du PC client doit être configurée pour DHCP car elle obtiendra une adresse IP dans la plage 169.254.x.y en environ 1 minute.
2. Démarrez un navigateur Web (ou bien une session telnet ou SSH), puis sélectionnez l'adresse IP du service Onboard Administrator telle qu'elle est affichée dans la fenêtre Enclosure Info de l'écran Insight Display.
3. À l'aide du mot de passe administrateur relié au module Onboard Administrator actif, connectez-vous au module Onboard Administrator en tant qu'administrateur.
4. Au cours de l'assistant First Time Setup, activez Device Bay EBIPA avec une adresse IP fixe et activez Interconnect Bay EBIPA avec une adresse IP différente de départ. Après l'exécution de l'assistant First Time Setup, vous pouvez à tout moment modifier les paramètres EBIPA en sélectionnant **Enclosure Bay IP Addressing** dans la liste Enclosure Settings.

Cliquer sur le bouton **Autofill** (Remplissage auto) crée autant d'adresses IP fixes séquentielles que nécessaire. Le masque de sous réseau, la passerelle, les serveurs DNS, les serveurs NTP et le nom de domaine sont également copiés dans chacune des baies consécutives de la liste. Alternativement, vous pouvez attribuer manuellement des adresses IP fixes individuelles en entrant l'adresse IP souhaitée dans le champ d'adresse EBIPA pour la baie spécifique. Le masque de sous réseau, la passerelle, les serveurs DNS et le domaine peuvent être identiques ou différents pour chaque baie.

Après avoir appliqué les paramètres, les serveurs dans les baies de périphérique vont obtenir automatiquement les adresses EBIPA de baies de périphérique en quelques minutes, mais les modules commutateurs d'interconnexion doivent être redémarrés manuellement en cliquant sur le bouton **Virtual Power** (Alimentation virtuelle) dans chaque page d'informations du module d'interconnexion Onboard Administrator.

5. Pour vérifier que les adresses iLO de lame de serveur ont été définies selon l'adresse IP de début EBIPA et la plage, utilisez la liste de périphériques Onboard Administrator.

Écran IPv4 EBIPA de l'assistant First Time Setup


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
First Time Setup Wizard
Set up initial enclosure and server settings
Step 7.1 of 13
Welcome
FIPS
Enclosure Selection
Configuration Management
Rack and Enclosure Settings
Administrator Account Setup
Local User Accounts
Enclosure Bay IP Addressing
IPv4
IPv6
Directory Groups
Directory Settings
Onboard Administrator Network Settings
SNMP Settings
Power Management
Finish
IPv4
Device Bay iLO Processor Address Range: The form below provides fixed IP address assignment to the device bays in the enclosure. If there is an IP address in the Current Address column, the device (iLO) has previously been configured or has received a DHCP address.
Note: All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IP address, these EBIPA settings will not change th static IP address. If the iLO IP address has been configured via an external DHCP service, the EBIPA settings will override the existing DHCP address.
When EBIPA is configured the network is checked for duplicate IP addresses. This process may take several minutes, especially if multiple enclosures have been selected.
Device List: This list displays the IP addresses that will be assigned to each of the device bays if EBIPA is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IP addresses for all of the device bays below the arrow. The subnet mask, gateway, domain, and DNS servers will also be copied to each of the consecutive bays in the list.
Bay
Enabled
EBIPA Address
Subnet Mask
Gateway
Domain
DNS Servers
Autofill
Current Address
1
16.84.195.125
2
16.84.193.89
3
N/A
4
N/A
5
16.84.194.209

REMARQUE : N'utilisez pas la plage 169.254.x.x lors de la configuration de l'attribution des adresses EBIPA, car cette plage d'adresses réseau est réservée à l'usage du module Onboard Administrator.

Liste des périphériques

Colonne	Description
Bay (Baie)	Baie dans le boîtier du périphérique.
Enabled (Activé)	Active les paramètres EBIPA pour la baie de périphérique. Les paramètres EBIPA pour toutes les baies de périphériques peuvent être activés par la sélection de la case à cocher en regard de Enabled (Activé) dans la rangée d'en-tête ou des baies de périphériques individuelles peuvent

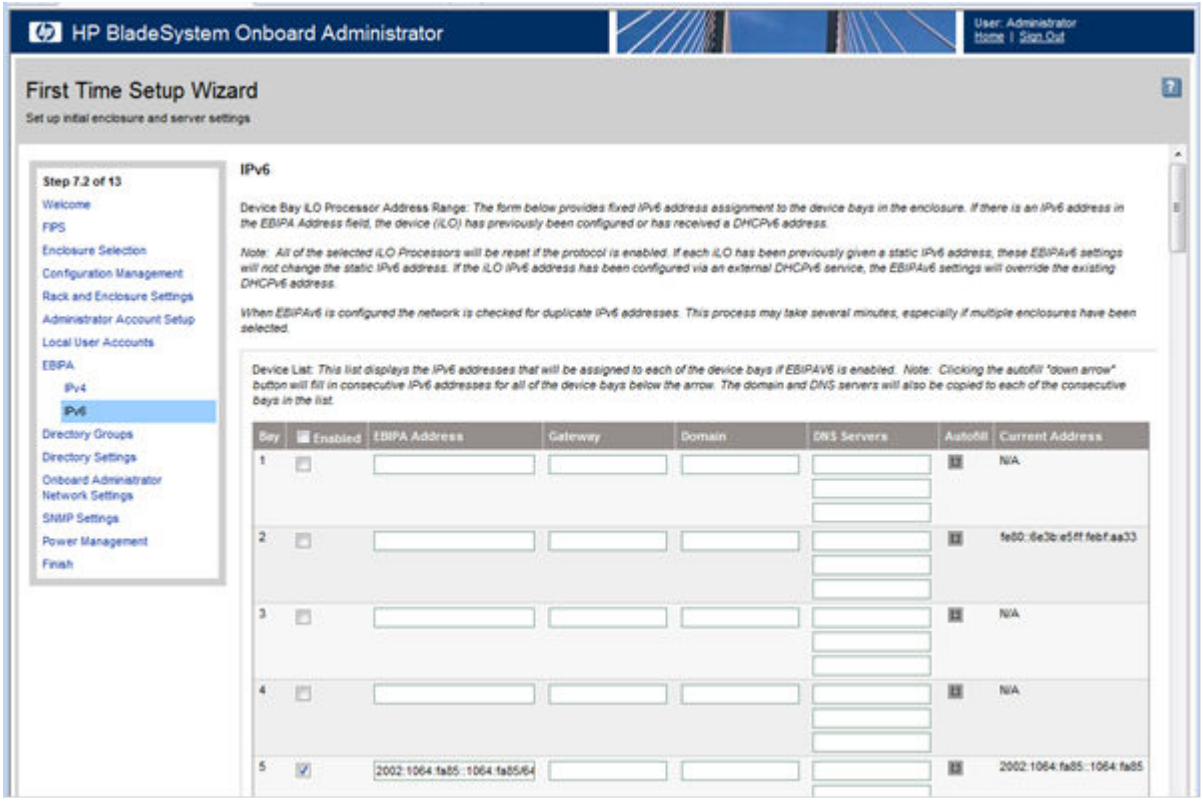
Colonne	Description
	être sélectionnées en cochant la case pour cette baie de périphérique donnée.
EBIPA Address (Adresse EBIPA)	Adresse IP fixe à affecter à la baie de périphérique. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Subnet Mask (Masque de sous-réseau)	Masque de sous-réseau des baies de périphérique. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Gateway (Passerelle)	Adresse IP de passerelle fixe à affecter à la baie de périphérique. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Domain (Domaine)	Nom de domaine des baies de périphérique. Les valeurs possibles sont une chaîne de caractères comprenant au maximum 64 caractères, y compris tous les caractères alphanumériques, le tiret (-) et le point (.).
DNS Servers (Serveurs DNS)	Adresses IP des serveurs DNS principal, secondaire et tertiaire. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Autofill (Remplissage auto)	Affecte des adresses IP consécutives pour les baies de périphériques sélectionnées au-dessous de la liste de périphériques. Pour attribuer les adresses IP, cliquez sur la flèche vers le bas **Autofill**. Le bouton Autofill (Remplissage auto) ne remplit que tous les champs d'adresse si le champ d'adresse associé à la première adresse de la liste est sélectionné. Par exemple, le remplissage automatique de l'adresse 1 remplira les adresses 1 à 16, le remplissage automatique de l'adresse 2 remplira les adresses 2 à 16, etc. Lors de l'utilisation du remplissage automatique, spécifiez un masque de sous-réseau IPv4 qui autorise suffisamment d'adresses disponibles sur le sous-réseau associé pour remplir tous les champs d'adresse correspondant au nombre total de baies sélectionnées. Si vous spécifiez un masque de sous-réseau qui ne répond pas à cette exigence, « Invalid IP Address » (Adresse IP non valide) s'affiche dans le champ d'adresse de chaque baie pour laquelle une adresse ne peut pas être générée.
Current Address (Adresse actuelle)	Adresse IP actuelle de la baie de périphérique.

Liste d'interconnexion

Colonne	Description
Bay (Baie)	Baie dans le boîtier du périphérique d'interconnexion.
Enabled (Activé)	Active les paramètres EBIPA pour IPv4 pour la baie d'interconnexion. Les paramètres EBIPA pour IPv4 pour toutes les baies d'interconnexion peuvent être activés par la sélection de la case à cocher en regard de Enabled (Activé) dans la rangée d'en-tête ou des baies d'interconnexion individuelles peuvent être sélectionnées en cochant la case pour cette baie d'interconnexion donnée.

Colonne	Description
EBIPA Address (Adresse EBIPA)	Adresse IP DHCP statique à affecter à la baie de périphérique.
Subnet Mask (Masque de sous-réseau)	Masque de sous-réseau des baies de périphérique. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Gateway (Passerelle)	Adresse de passerelle des baies de périphérique. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Domain (Domaine)	Nom de domaine des baies de périphérique. Les valeurs possibles sont une chaîne de caractères comprenant au maximum 64 caractères, y compris tous les caractères alphanumériques, le tiret (-) et le point (.).
DNS Servers (Serveurs DNS)	Adresses IPv4 des serveurs DNS principal, secondaire et tertiaire. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
NTP Server (Serveur NTP)	Adresse IPv4 du serveur utilisée pour la synchronisation de la date et de l'heure à l'aide du protocole NTP. ###.###.###.### où ### est compris entre 0 et 255
Autofill (Remplissage auto)	Affecte des adresses IPv4 consécutives pour les baies d'interconnexion sélectionnées au-dessous de la liste d'interconnexion. Pour attribuer les adresses IP, cliquez sur la flèche vers le bas **Autofill**. Le bouton Autofill (Remplissage auto) ne remplit que tous les champs d'adresse si le champ d'adresse associé à la première adresse de la liste est sélectionné. Par exemple, le remplissage automatique de l'adresse 1 remplira les adresses 1 à 16, le remplissage automatique de l'adresse 2 remplira les adresses 2 à 16, etc. Lors de l'utilisation du remplissage automatique, spécifiez un masque de sous-réseau IPv4 qui autorise suffisamment d'adresses disponibles sur le sous-réseau associé pour remplir tous les champs d'adresse correspondant au nombre total de baies sélectionnées. Si vous spécifiez un masque de sous-réseau qui ne répond pas à cette exigence, « Invalid IP Address » (Adresse IP non valide) s'affiche dans le champ d'adresse de chaque baie pour laquelle une adresse ne peut pas être générée.
Current Address (Adresse actuelle)	Adresse IPv4 actuelle de la baie d'interconnexion.

Écran IPv6 EBIPA de l'assistant First Time Setup


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
First Time Setup Wizard
Set up initial enclosure and server settings
Step 7.2 of 13
Welcome
FIPS
Enclosure Selection
Configuration Management
Rack and Enclosure Settings
Administrator Account Setup
Local User Accounts
EBIPA
IPv4
IPv6
Directory Groups
Directory Settings
Onboard Administrator Network Settings
SNMP Settings
Power Management
Finish
IPv6
Device Bay iLO Processor Address Range: The form below provides fixed IPv6 address assignment to the device bays in the enclosure. If there is an IPv6 address in the EBIPA Address field, the device (iLO) has previously been configured or has received a DHCPv6 address.
Note: All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IPv6 address, these EBIPAv6 settings will not change the static IPv6 address. If the iLO IPv6 address has been configured via an external DHCPv6 service, the EBIPAv6 settings will override the existing DHCPv6 address.
When EBIPAv6 is configured the network is checked for duplicate IPv6 addresses. This process may take several minutes, especially if multiple enclosures have been selected.
Device List: This list displays the IPv6 addresses that will be assigned to each of the device bays if EBIPAV6 is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the device bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.
Bay
Enabled
EBIPA Address
Gateway
Domain
DNS Servers
Autofill
Current Address
1
N/A
2
fe80::6e3b:e5ff:feb:aa33
3
N/A
4
N/A
5
2002:1064:fa85::1064:fa85/64
2002:1064:fa85::1064:fa85

REMARQUE : N'utilisez pas le préfixe fe80::/10 lors de la configuration de l'attribution des adresses EBIPA : ce préfixe réseau est réservé aux adresses SLAAC de liens locaux.

REMARQUE : Pour que les adresses fixées par IPv6 EBIPA soient configurées avec succès, le paramètre **Enable IPv6** doit être activé. Pour activer ce paramètre, utilisez l'écran First Time Setup Wizard Network IPv6 Settings ou l'onglet Enclosure Settings IPv6 Settings.

Les paramètres **Enable SLAAC** (Activer SLAAC) et **Enable DHCPv6** (Activer DHCPv6) n'ont aucun effet sur la fonctionnalité IPv6 EBIPA.

Liste des périphériques

Colonne	Description
Bay (Baie)	Baie dans le boîtier du périphérique.
Enabled (Activé)	Active les paramètres EBIPA pour la baie de périphérique. Les paramètres EBIPA pour toutes les baies de périphériques peuvent être activés par la sélection de la case à cocher en regard de Enabled (Activé) dans la rangée d'en-tête ou des baies de périphériques individuelles peuvent être sélectionnées en cochant la case pour cette baie de périphérique donnée.
EBIPA Address (Adresse EBIPA)	Adresse IPv6 fixe à affecter à la baie de périphérique. Les valeurs possibles sont ####:####:####:####:####:####:####:####/###, où #### est compris entre 0 et FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. Les plages de préfixe /### compris entre 1 et 128 ; la longueur du préfixe est obligatoire.

Colonne	Description
Gateway (Passerelle)	Adresse de passerelle IPv6 fixe à affecter à la baie de périphérique. Les valeurs possibles sont ####:####:####:####:####:####:####:#### où #### est compris dans la plage de 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. Ne spécifiez pas de préfixe. La passerelle est supposée être accessible au sein du réseau. Si cette passerelle est spécifiée comme une adresse de liaison locale, la passerelle sera toujours configurée sur le périphérique de boîtier utilisant cette adresse. Si la passerelle est spécifiée avec tout autre type d'adresse IPv6, le module Onboard Administrator envoie des demandes de sollicitation à caractère voisin pour identifier l'adresse de liaison locale du périphérique de passerelle pour une utilisation dans le périphérique du boîtier. Si la passerelle n'existe pas ou ne répond pas aux demandes de sollicitation à caractère voisin, aucune passerelle n'est configurée.
Domain (Domaine)	Nom de domaine des baies de périphérique. Les valeurs possibles sont une chaîne de caractères comprenant au maximum 64 caractères, y compris tous les caractères alphanumériques, le tiret (-) et le point (.).
DNS Servers (Serveurs DNS)	Adresses IPv6 des serveurs DNS principal, secondaire et tertiaire. Les valeurs possibles sont ####:####:####:####:####:####:####:#### où #### est compris dans la plage de 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge.
Autofill (Remplissage auto)	Affecte des adresses IPv6 consécutives pour les baies de périphériques sélectionnées au-dessous de la liste de périphériques. Pour attribuer les adresses IP, cliquez sur la flèche vers le bas **Autofill**. Le bouton Autofill (Remplissage auto) ne remplit que tous les champs d'adresse si le champ d'adresse associé à la première adresse de la liste est sélectionné. Par exemple, le remplissage automatique de l'adresse 1 remplira les adresses 1 à 16, le remplissage automatique de l'adresse 2 remplira les adresses 2 à 16, etc. Lors de l'utilisation du remplissage automatique, spécifiez un préfixe de sous-réseau IPv6 qui autorise suffisamment d'adresses disponibles sur le sous-réseau associé pour remplir tous les champs d'adresse correspondant au nombre total de baies sélectionnées. Si vous spécifiez un préfixe ou un masque de sous-réseau qui ne répond pas à cette exigence, « Invalid IP Address » (Adresse IP non valide) s'affiche dans le champ d'adresse de chaque baie pour laquelle une adresse ne peut pas être générée.
Current Address (Adresse actuelle)	Adresse IPv6 actuelle de la baie de périphérique.

Liste d'interconnexion

Colonne	Description
Bay (Baie)	Baie dans le boîtier du périphérique d'interconnexion.
Enabled (Activé)	Active les paramètres EBIPA pour IPv6 pour la baie d'interconnexion. Les paramètres EBIPA pour IPv6 pour

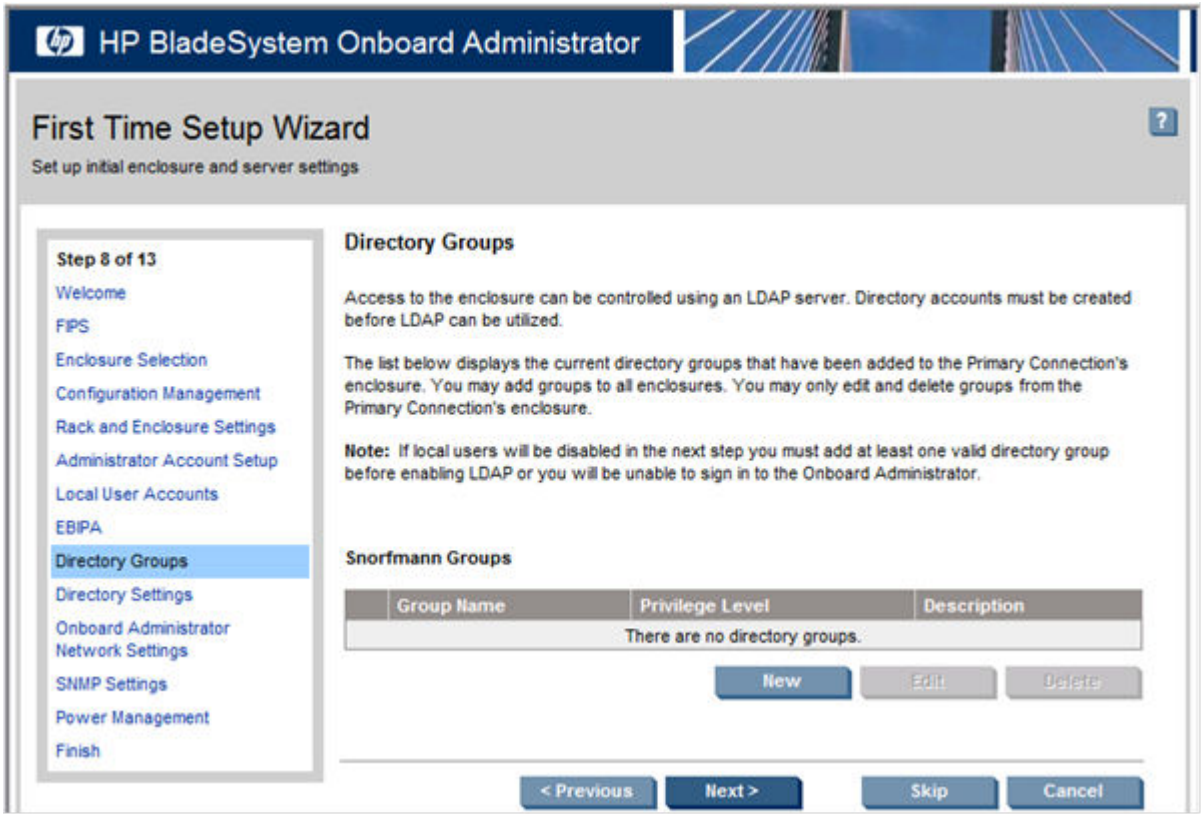
Colonne	Description
	toutes les baies d'interconnexion peuvent être activés par la sélection de la case à cocher en regard de Enabled (Activé) dans la rangée d'en-tête ou des baies d'interconnexion individuelles peuvent être sélectionnées en cochant la case pour cette baie d'interconnexion donnée.
EBIPA Address (Adresse EBIPA)	Adresse IP IPv6 DHCP fixe à affecter à la baie d'interconnexion. Les valeurs possibles sont ####:####:####:####:####:####:####:####/###, où #### est compris entre 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. Les plages de préfixe /### compris entre 1 et 128 ; la longueur du préfixe est obligatoire.
Gateway (Passerelle)	Adresse IPv6 de passerelle fixe à affecter à la baie d'interconnexion. Les valeurs possibles sont ####:####:####:####:####:####:####:#### où #### est compris dans la plage de 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. Ne spécifiez pas de préfixe. La passerelle est supposée être accessible au sein du réseau. Si cette passerelle est spécifiée comme une adresse de liaison locale, la passerelle sera toujours configurée sur le périphérique de boîtier utilisant cette adresse. Si la passerelle est spécifiée avec tout autre type d'adresse IPv6, le module Onboard Administrator envoie des demandes de sollicitation à caractère voisin pour identifier l'adresse de liaison locale du périphérique de passerelle pour une utilisation dans le périphérique du boîtier. Si la passerelle n'existe pas ou ne répond pas aux demandes de sollicitation à caractère voisin, aucune passerelle n'est configurée.
Domain (Domaine)	Nom de domaine des baies de périphérique. Les valeurs possibles sont une chaîne de caractères comprenant au maximum 64 caractères, y compris tous les caractères alphanumériques, le tiret (-) et le point (.).
DNS Servers (Serveurs DNS)	Adresses IPv6 des serveurs DNS principal, secondaire et tertiaire. Les valeurs possibles sont ####:####:####:####:####:####:####:####, où #### est compris entre 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge.
Autofill (Remplissage auto)	Affecte des adresses IPv6 consécutives pour les baies d'interconnexion sélectionnées au-dessous de la liste d'interconnexion. Pour attribuer les adresses IP, cliquez sur la flèche vers le bas **Autofill**. Le bouton Autofill (Remplissage auto) ne remplit que tous les champs d'adresse si le champ d'adresse associé à la première adresse de la liste est sélectionné. Par exemple, le remplissage automatique de l'adresse 1 remplira les adresses 1 à 16, le remplissage automatique de l'adresse 2 remplira les adresses 2 à 16, etc. Lors de l'utilisation du remplissage automatique, spécifiez un préfixe de sous-réseau IPv6 qui autorise suffisamment d'adresses disponibles sur le sous-réseau associé pour remplir tous les champs d'adresse correspondant au nombre total de baies sélectionnées. Si vous spécifiez un préfixe ou un masque de sous-réseau qui ne répond pas à cette exigence, « Invalid IP Address » (Adresse IP non valide)

Colonne	Description
	s'affiche dans le champ d'adresse de chaque baie pour laquelle une adresse ne peut pas être générée.
Current Address (Adresse actuelle)	Adresse IPv6 actuelle de la baie d'interconnexion.

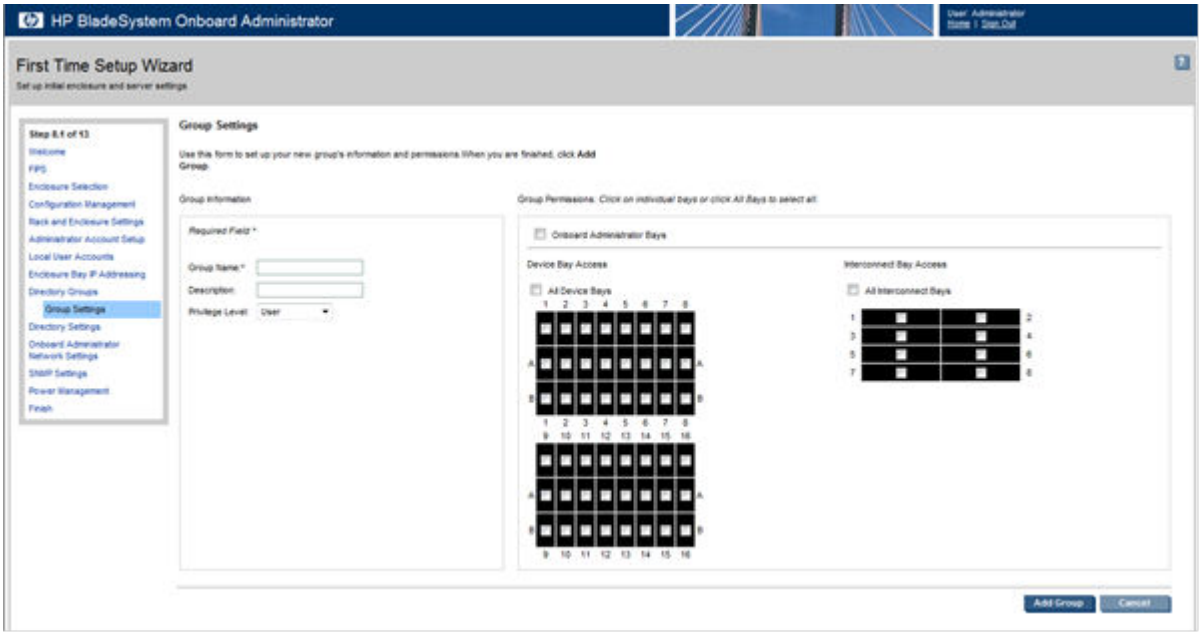
Écran Directory Group Configuration

LDAP est un protocole ouvert d'accès aux annuaires d'information. Bien que le protocole LDAP soit basé sur la norme X.500, il est bien plus simple. LDAP prend en charge le protocole TCP/IP afin de permettre à des applications de fonctionner indépendamment du serveur qui héberge l'annuaire.

L'illustration suivante représente l'écran Directory Groups de l'assistant First Time Setup, qui ermet d'ajouter, de modifier et de supprimer des groupes d'annuaire :


HP BladeSystem Onboard Administrator
First Time Setup Wizard
Set up initial enclosure and server settings
Step 8 of 13
Welcome
FIPS
Enclosure Selection
Configuration Management
Rack and Enclosure Settings
Administrator Account Setup
Local User Accounts
EBIPA
Directory Groups
Directory Settings
Onboard Administrator Network Settings
SNMP Settings
Power Management
Finish
Directory Groups
Access to the enclosure can be controlled using an LDAP server. Directory accounts must be created before LDAP can be utilized.
The list below displays the current directory groups that have been added to the Primary Connection's enclosure. You may add groups to all enclosures. You may only edit and delete groups from the Primary Connection's enclosure.
Note: If local users will be disabled in the next step you must add at least one valid directory group before enabling LDAP or you will be unable to sign in to the Onboard Administrator.
Snorfmann Groups
Group Name
Privilege Level
Description
There are no directory groups.
New
Edit
Delete
< Previous
Next >
Skip
Cancel

Pour ajouter un groupe d'annuaires, cliquez sur **New** (Nouveau). La figure suivante illustre l'écran de paramètres de groupe de l'assistant de première configuration qui permet de configurer un nouveau groupe d'annuaires et de définir l'accès aux annuaires pour les boîtiers sélectionnés.



L'accès au boîtier peut être accordé en utilisant LDAP. Pour utiliser le serveur LDAP, vous devez créer des comptes d'annuaire.

L'écran Directory Groups affiche les groupes d'annuaires actuels qui ont été ajoutés au boîtier de la connexion principale. Vous pouvez ajouter des groupes d'utilisateurs à tous les boîtiers. Vous pouvez modifier et supprimer des groupes d'utilisateurs uniquement du boîtier de connexion principale. Pour utiliser les services LDAP, vous devez ajouter au moins un groupe d'annuaires.

Colonne	Description
Case à cocher	Permet de sélectionner un groupe d'annuaires pour modification ou suppression.
Group Name (Nom de groupe)	De 1 à 255 caractères. Contient les mêmes caractères que les contextes de recherche. Le nom de groupe est utilisé pour déterminer l'appartenance à un groupe d'utilisateurs LDAP. Le nom de groupe doit correspondre à l'une des cinq propriétés suivantes d'un groupe d'annuaires : le nom, le nom unique, le nom commun, le nom d'affichage ou le nom de compte SAM. Pour les groupes imbriqués, la correspondance est basée sur `objectSid` (un attribut qui spécifie l'identifiant de sécurité du groupe). Le nom unique est recommandé pour spécifier uniquement le groupe LDAP. Si le module Onboard Administrator est configuré pour rechercher le port GC et si un nom unique n'est pas utilisé, alors une correspondance incorrecte dans plusieurs domaines peut se produire pour entraîner une autorisation involontaire.
Privilege Level (Niveau de privilège)	Utilisé pour déterminer les fonctions d'administration que l'utilisateur est autorisé à exécuter. Le niveau de privilège d'un utilisateur peut être administrateur, opérateur ou utilisateur.
Description	De 0 à 58 caractères, y compris les caractères alphanumériques, le tiret (-), le trait de soulignement (_) et l'espace. Description du groupe LDAP, une version plus lisible du nom de groupe, ou d'autres informations utiles.

- **New** (Nouveau) : cliquez sur le bouton **New** pour ajouter un nouvel groupe d'annuaires au boîtier sélectionné. Vous pouvez ajouter un maximum de 30 groupes d'annuaires. L'écran Add LDAP Group (Ajouter un groupe LDAP) s'affiche.
- **Edit** (Modifier) : sélectionnez un groupe d'annuaires à modifier en activant la case à cocher en regard du nom du groupe. Pour modifier les paramètres dans l'écran Edit LDAP Group (Modification du groupe LDAP), cliquez sur **Edit** (Modifier).
- **Delete** (Supprimer) : sélectionnez le groupe d'annuaires à supprimer en activant la case à cocher en regard du nom du groupe. Pour supprimer le groupe, cliquez sur **Delete** (Supprimer).

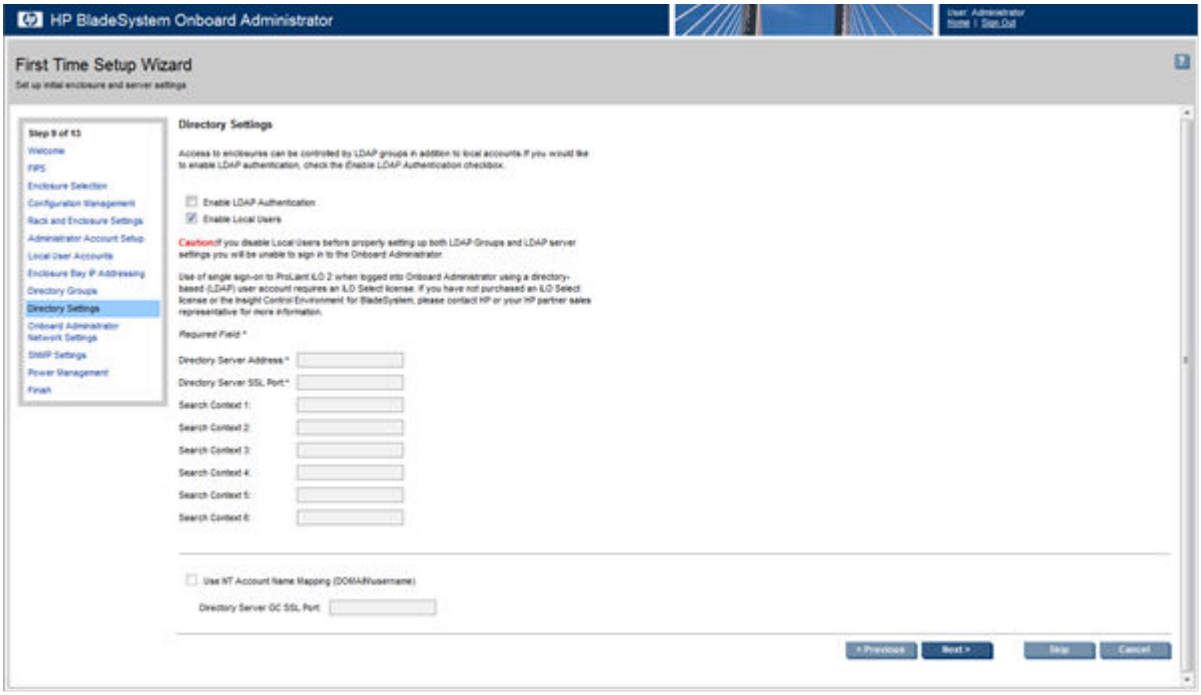
Prise en charge de groupe LDAP imbriqué

Lorsque vous utilisez Microsoft Active Directory, vous pouvez placer un ou plusieurs groupes dans un autre groupe. Les groupes qui sont contenus dans un autre groupe sont appelés des groupes imbriqués. Le groupe qui contient des groupes imbriqués est appelé un groupe d'imbrication. L'avantage des groupes imbriqués est de pouvoir connecter les utilisateurs d'un groupe imbriqué au module Onboard Administrator si leur groupe d'imbrication est correctement configuré. Par exemple, supposons que `group2` est imbriqué dans `group1`. Les utilisateurs de `group2` sont autorisés à se connecter au module Onboard Administrator si le groupe LDAP parent (`group1`) est ajouté au module Onboard Administrator et peut être trouvé en utilisant l'un des contextes de recherche. Le contexte de la recherche ne se limite pas à l'emplacement exact : si le chemin de contexte de recherche est élevé dans l'arborescence de l'annuaire LDAP, la recherche de sous-arbre est utilisée. Le module Onboard Administrator ne prend en charge que le type de groupe de sécurité. Le type de groupe de distribution n'est pas pris en charge.

Pour appliquer les paramètres, cliquez sur **Next** (Suivant).

Écran Directory Settings

Utilisez l'écran Directory Settings suivant pour définir l'accès aux annuaires pour les boîtiers actuellement sélectionnés :



REMARQUE : La fonction LDAP du module Onboard Administrator prend en charge Microsoft® Active Directory à l'aide de l'attribut `memberOf`. Novell eDirectory est également pris en charge avec l'attribut `groupMembership`. OpenLDAP n'est pas pris en charge.

Cet écran permet de configurer les paramètres suivants :

- **Enable LDAP Authentication** (Activer l'authentification LDAP) : cochez cette case pour permettre à un serveur d'annuaire d'authentifier une connexion d'utilisateur.
- **Enable Local Users** (Activer les utilisateurs locaux) : cochez cette case pour permettre à un utilisateur de se connecter via un compte utilisateur local et non un compte d'annuaire.
- **Search Context** (Contexte de recherche) : spécifiez un à six contextes de recherche. Un contexte de recherche est un filtre de recherche ou un raccourci vers un annuaire commun, définissant le début de la recherche de l'utilisateur d'annuaire à l'emplacement spécifié. En spécifiant un contexte de recherche, les utilisateurs n'ont pas à indiquer leurs DN complets lors de la connexion. Un DN peut être long, et les utilisateurs peuvent ne pas connaître leurs DN ou peuvent avoir des comptes dans différents contextes d'annuaire. Le module Onboard Administrator tente de contacter le service d'annuaire par DN, puis applique les contextes de recherche dans l'ordre, en commençant par `Search Context 1` et continue à travers tous les contextes de recherche suivants jusqu'à la réussite.
  - **Exemple 1** :

    Supposons que vous êtes `user1`. Si vous entrez le contexte de recherche `ou=OU1,dc=hp,dc=com`, vous pouvez vous connecter en tant que `user1` au lieu de `cn=user1,ou=OU1,dc=hp,dc=com`.
  - **Exemple 2** :

    Supposons que les contextes de recherche suivants sont définis :
    - Contexte de recherche 1 : `ou=OU1,dc=hp,dc=com`
    - Contexte de recherche 2 : `ou=OU2,ou=OU1,dc=hp,dc=com`

    Si deux utilisateurs disposent du même nom commun `user1` dans deux contextes de recherche, et que leurs mots de passe sont identiques, lorsque l'utilisateur tente de se connecter, le module Onboard Administrator contacte `cn=user1,ou=OU1,dc=hp,dc=com`.

    Si les mots de passe sont différents et qu'un utilisateur fournit le mot de passe de l'utilisateur dans `OU2`, le module Onboard Administrator utilise DN `cn=user1,ou=OU1,dc=hp,dc=com`, mais il sera rejeté parce que le mot de passe ne correspond pas. La prochaine connexion sera tentée avec `cn=user1,ou=OU2,ou=OU1,dc=hp,dc=com`, avec succès.

Le contexte de recherche est également applicable aux groupes d'annuaires, qui sont utiles lorsque des groupes imbriqués LDAP sont configurés. Lorsque vous spécifiez le contexte de recherche pour un groupe d'annuaire LDAP, le contexte exact n'est pas nécessaire. Par exemple, si un emplacement de groupe est ou=OU2,ou=OU1,dc=hp,dc=com, le contexte de recherche de niveau supérieur ou=OU1,dc=hp,dc=com peut être utilisé pour localiser ce groupe. Cette fonction permet de contourner la limite de longueur des contextes de recherche. Pour plus d'informations sur les groupes imbriqués, consultez la section « Écran Directory Group Configuration » (Écran Directory Group Configuration à la page 73).

Champ	Valeur possible	Description
Directory Server Address (Adresse du serveur d'annuaire)	Adresse IPv4 : ###.###.###.### où ### est compris dans une plage de 0 à 255 ou nom DNS du serveur d'annuaire ou nom du domaine. Adresse Ipv6 : ####:####:####:####:####:####:####:####, où #### est compris entre 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge.	Adresse IP, nom DNS ou nom du domaine du service d'annuaire. Ce champ est obligatoire.
Directory Server SSL Port (Port SSL du serveur d'annuaire)	1 à 65535	Port utilisé pour les communications LDAP. Le port 636 est le port LDAP SSL standard. Ce champ est obligatoire.
Search Context 1 (Contexte de recherche 1)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Premier chemin de recherche utilisé pour localiser l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.
Search Context 2 (Contexte de recherche 2)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Deuxième chemin de recherche utilisé pour localiser l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.
Search Context 3 (Contexte de recherche 3)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Troisième chemin de recherche utilisé pour localiser l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.
Search Context 4 (Contexte de recherche 4)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Quatrième chemin de recherche utilisé pour repérer l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.
Search Context 5 (Contexte de recherche 5)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Cinquième chemin de recherche utilisé pour repérer l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.
Search Context 6 (Contexte de recherche 6)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Sixième chemin de recherche utilisé pour repérer l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est

Champ	Valeur possible	Description
		également utilisé pour rechercher un groupe d'imbrication LDAP.

- **Use NT Account Name Mapping (DOMAIN\username)** (Utiliser le mappage de noms de comptes NT (DOMAINE\nom d'utilisateur)) : cochez cette case pour permettre le mappage de noms NT. Ce champ permet aux utilisateurs de se connecter en utilisant le format NT `domaine\nom_utilisateur`. Le module Onboard Administrator peut être configuré en option pour rechercher le Catalogue mondial du serveur d'annuaire et localiser les informations de l'utilisateur authentifié et des groupes autorisés associés. Le port GC SSL standard du serveur d'annuaire est 3269. Ce champ est facultatif et, s'il reste vierge, le catalogue mondial n'est pas utilisé.

REMARQUE : Si le mappage de noms de comptes NT est utilisé avec le catalogue mondial et que le contexte de recherche n'est pas assez restrictif, ou bien que le nom du domaine n 'est pas spécifié, le module Onboard Administrator peut associer l'utilisateur authentifié à un compte utilisateur qui a le même nom dans un domaine différent. L'utilisateur authentifié recevrait alors l'autorisation de l'utilisateur dans l'autre domaine. Pour éviter toute ambigüité lors de la connexion de l'utilisateur LDAP, sélectionnez les contextes de recherche ou fournissez le nom du domaine.

REMARQUE : Si le mappage de noms de comptes NT est utilisé avec le catalogue mondial et ne peut pas être résolu avec un utilisateur unique, l'utilisateur n'est pas autorisé à accéder au module Onboard Administrator. Cela peut se produire avec des contextes de recherche qui ne sont pas assez restrictifs et si plusieurs comptes ayant le même nom existent dans différents domaines. Pour éviter toute ambigüité, sélectionnez les contextes de recherche.

REMARQUE : Les règles de mot de passe appliquées sur les serveurs LDAP pourraient être différentes des règles de mot de passe appliquées pour les comptes utilisateur locaux. Assurez-vous que les deux ensembles de règles adhèrent aux politiques de sécurité.

Pour appliquer les paramètres, cliquez sur **Next** (Suivant).

Écran Onboard Administrator Network Settings

Onboard Administrator Network Settings

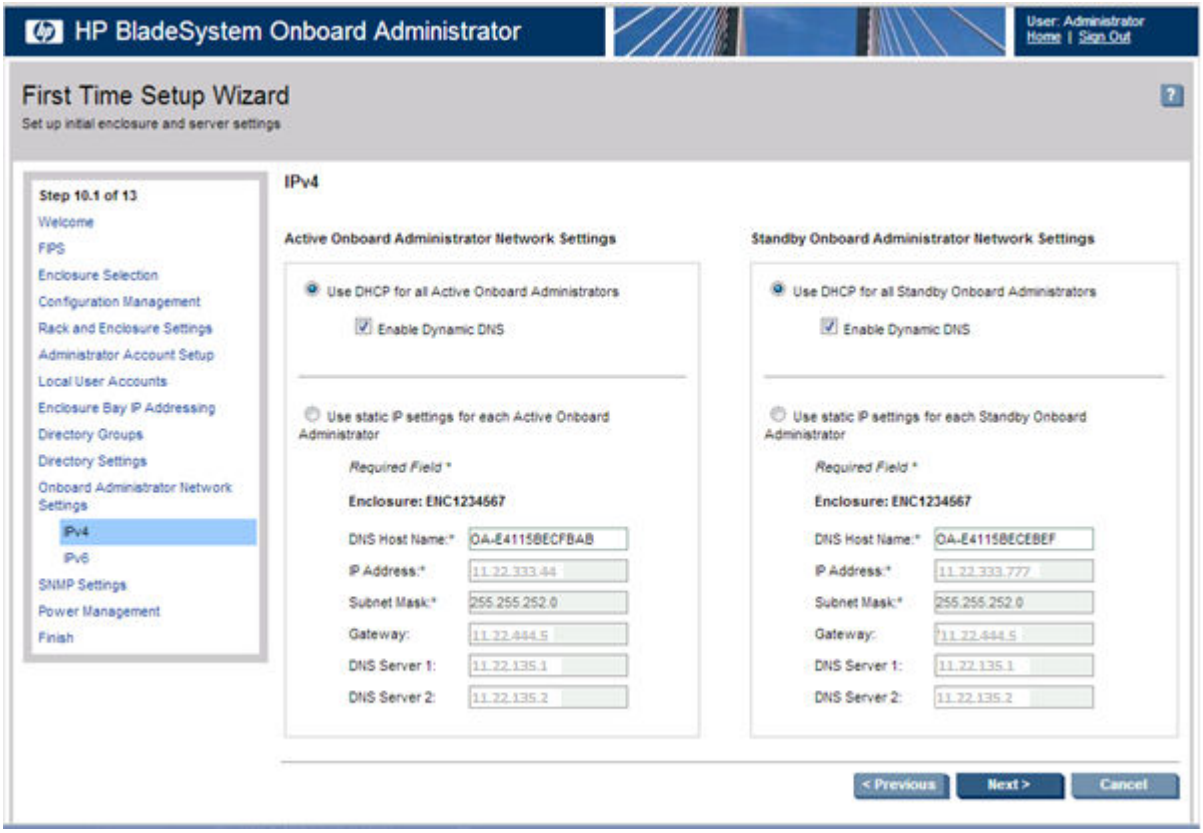
Pour modifier les paramètres réseau des modules Onboard Administrator dans les boîtiers sélectionnés, utilisez les écrans Onboard Administrator Network Settings IPv4 ou IPv6. Chaque écran permet de configurer les paramètres réseau du module Onboard Administrator actif et du module Onboard Administrator en Standby. Les paramètres des modules Onboard Administrator en mode Standby s'affichent uniquement si les modules sont présents.

La modification de paramètres réseau sur le module Onboard Administrator auquel vous êtes connecté peut vous déconnecter du module Onboard Administrator, auquel cas, après l'application des paramètres, vous devrez vous reconnecter au module Onboard Administrator.

Pour continuer, cliquez sur **Next** (Suivant).

Si vous ne souhaitez pas modifier de paramètres réseau, cliquez sur **Skip** (Ignorer).

Écran des paramètres réseau IPv4 de l'assistant First Time Setup



Paramètres réseau IPv4 de l'assistant First Time Setup

Le module Onboard Administrator permet de baser la configuration du réseau IPv4 sur des adresses IP attribuées dynamiquement obtenues à partir d'un serveur DHCP ou sur des adresses IP statiques que vous spécifiez manuellement. Vous choisissez la base de la configuration du réseau en sélectionnant la case d'option appropriée. Si vous choisissez DHCP, vous pouvez activer DNS dynamique.

- **Use DHCP for all Active (or Standby) Onboard Administrator** (Utiliser DHCP pour tous les modules Onboard Administrator actifs [ou en Standby]) : permet d'obtenir l'adresse IP du module Onboard Administrator à partir d'un serveur DHCP. La case à cocher Standby est uniquement affichée si un module Onboard Administrator en Standby est présent dans le boîtier.
- **Enable Dynamic DNS** (Activer DNS dynamique) : permet d'utiliser le même nom d'hôte pour le module Onboard Administrator au fil du temps, bien que l'adresse IP attribuée dynamiquement puisse changer. Le nom d'hôte est inscrit avec un serveur DNS. DDNS met à jour le serveur DNS avec des enregistrements nouveaux ou modifiés pour les adresses IP.

  La désactivation de DNS dynamique sur le module Onboard Administrator arrête les mises à jour du module Onboard Administrator vers le serveur DNS. Toutefois, notez que certains serveurs DHCP peuvent disposer d'une clause pour mettre à jour des serveurs DNS directement. Pour désactiver totalement les mises à jour de DNS dynamique, désactivez le service DNS dynamique au niveau du module Onboard Administrator ainsi que sur le serveur DHCP.
- **Use static IP settings for each Active (or Standby) Onboard Administrator** (Utiliser des paramètres d'adresse IP statique pour chaque module Onboard Administrator actif [ou en Standby]) : permet de définir manuellement des paramètres d'adresse IP statique pour le module Onboard Administrator. La case à cocher Standby est uniquement affichée si un module Onboard Administrator en Standby est présent dans le boîtier.

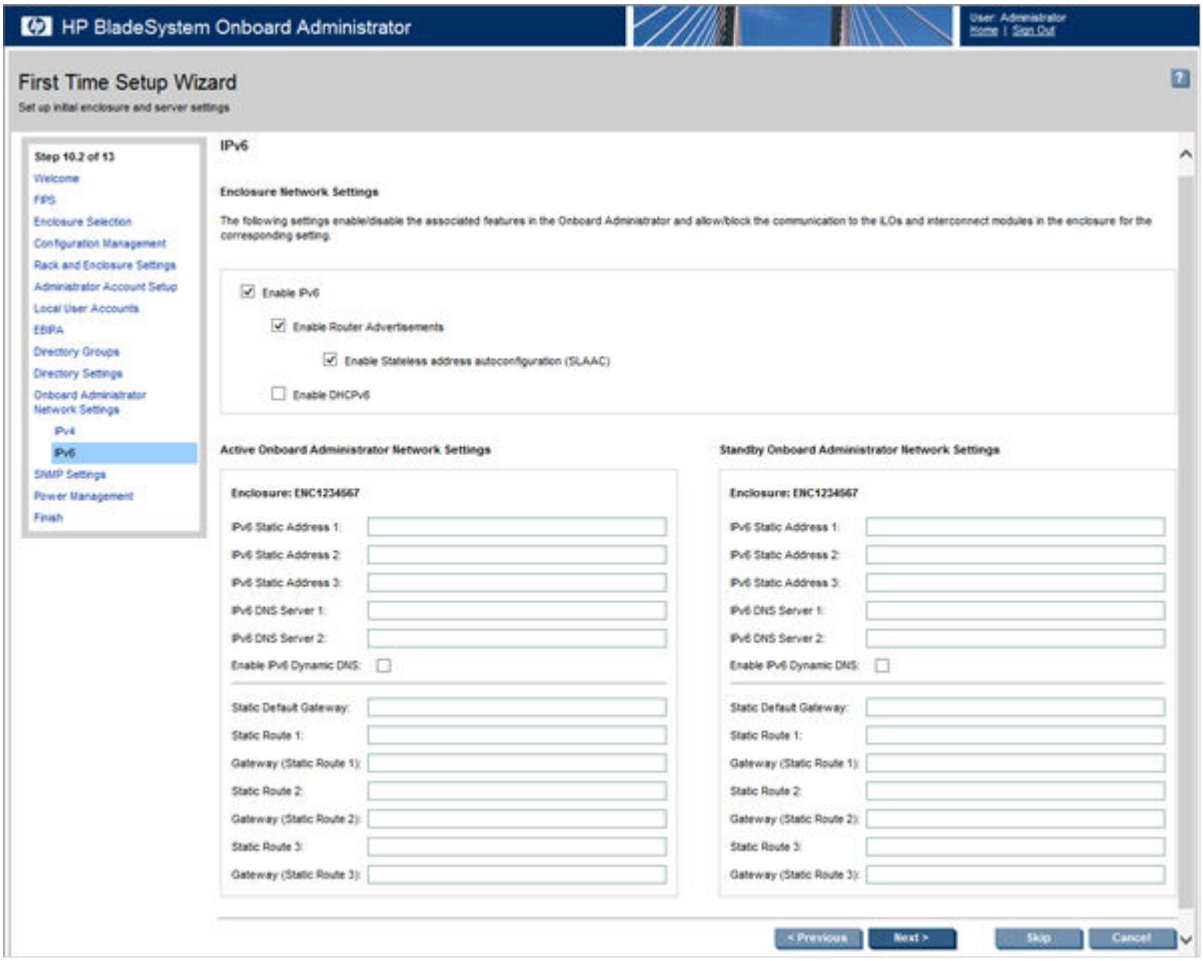
⚠ **ATTENTION :** Lors de l'activation de DHCP pour IPv4, tous les paramètres IPv4 statiques sont perdus.

Champ	Valeur possible	Description
DNS Host Name (Nom d'hôte DNS)	De 1 à 32 caractères, notamment tous les caractères alphanumériques, le tiret (-) et le trait de soulignement (_).	Le nom d'hôte DNS du module Onboard Administrator. Ce paramètre s'applique aux environnements à la fois IPv4 et IPv6. Le nom d'hôte DNS peut être attribué lorsque vous utilisez des paramètres IP statiques ou DHCP. La modification du nom de DNS Onboard Administrator peut provoquer une discordance de noms d'hôte sur le certificat SSL. Vous devrez peut-être mettre à jour les informations de certificat sur le module Onboard Administrator affecté, à l'aide de l'écran Active Onboard Administrator Certificate Administration (Onglet d'informations d'administration de certificat à la page 215) ou l'écran Standby Onboard Administrator Certificate Administration (Onglet Standby Onboard Administrator Certificate Administration Information à la page 232), selon les besoins.
IP Address (Adresse IP)	###.###.###.### où ### est compris entre 0 et 255	Adresse IP statique du module Onboard Administrator (requise si des paramètres IP statiques sont sélectionnés).
Subnet Mask (Masque de sous-réseau)	###.###.###.### où ### est compris entre 0 et 255	Masque de sous-réseau du module Onboard Administrator (requis si des paramètres IP statiques sont sélectionnés).
Gateway (Passerelle)	###.###.###.### où ### est compris entre 0 et 255	Adresse de passerelle du module Onboard Administrator (requise si des paramètres IP statiques sont sélectionnés).
DNS Server 1 (Serveur DNS 1)	###.###.###.### où ### est compris entre 0 et 255	Adresse IP du serveur DNS IPv4 principal.*
DNS Server 2 (Serveur DNS 2)	###.###.###.### où ### est compris entre 0 et 255	Adresse IP du serveur DNS IPv4 secondaire.*

* L'ordre dans lequel le module Onboard Administrator utilise des serveurs DNS est décrit dans l'onglet IPv4 Settings (Onglet IPv4 Settings à la page 126).

Pour enregistrer les nouveaux paramètres IPv4, cliquez sur **Next** (Suivant).

Écran des paramètres réseau IPv6 de l'assistant First Time Setup



Paramètres réseau IPv6 de l'assistant First Time Setup

IPv6 prend en charge plusieurs adresses. Vous pouvez activer n'importe quelle combinaison de paramètres réseau. Avec IPv6, SLAAC et/ou DHCPv6 activés, le module Onboard Administrator peut obtenir les adresses IP de toutes les sources sélectionnées. Il peut comporter des adresses IP attribuées automatiquement et des adresses IP statiques spécifiées par l'utilisateur. Les paramètres **Enable SLAAC**, **Enable DHCPv6** et **Enable Router Advertisements** prennent effet uniquement si IPv6 est activé.

- **Enable IPv6** (Activer IPv6) : active le protocole IPv6 pour tous les modules Onboard Administrator, les modules d'interconnexion et les modules iLO présents dans le boîtier.
- **Enable Router Advertisements** (Activer annonces de routeur) : autorise les annonces de routeur IPv6 à partir du réseau de gestion externe sur le réseau interne du boîtier. Si vous désactivez ce paramètre, le module Onboard Administrator bloque les annonces de routeur IPv6 envoyées du réseau de gestion externe, les empêchant d'entrer dans le réseau de gestion interne du boîtier.
- **Enable SLAAC** (Activer SLAAC) : active les messages de configuration automatique de l'adresse sans état IPv6 pour tous les modules Onboard Administrator, les modules d'interconnexion et les modules iLO du serveur présents dans le boîtier. Cette fonction ne concerne que les adresses IPv6 globales.
- **Enable DHCPv6** (Activer DHCPv6) : permet au module Onboard Administrator actif (et en veille, en cas de configuration adéquate) de demander une adresse IP DHCPv6. Autorise le trafic DHCPv6 sur le réseau de gestion du boîtier.

ATTENTION : Si vous désactivez IPv6 dans un environnement IPv6 uniquement, vous perdrez votre connexion à l'interface graphique du module Onboard Administrator et toutes les sessions SSH. Pour rétablir votre connexion, vous devez effectuer la configuration initiale du boîtier via les réseaux IPv4, Insight Display, ou l'interface de console série du module Onboard Administrator. Lors de la désactivation de IPv6, SLAAC ou DHCPv6, toutes les connexions qui dépendent du protocole désactivé sont fermées. Par exemple, si vous êtes connecté au module Onboard Administrator en utilisant son adresse attribuée par DHCPv6, la désactivation du paramètre DHCPv6 du boîtier résulte en la fermeture de votre session.

REMARQUE : Pour que des adresses SLAAC soient configurées avec succès, les paramètres **Enable SLAAC** et **Enable Router Advertisements** doivent être activés sur le boîtier. En outre, un routeur IPv6 doit être configuré sur le réseau de gestion du boîtier afin de fournir les adresses SLAAC via des annonces de routeur. Les cartes ILO peuvent doivent être configurées séparément pour obtenir des adresses SLAAC. Les paramètres **Enable SLAAC**, **Enable Router Advertisements** et **Enable IPv6** doivent être activés pour autoriser le trafic nécessaire sur le réseau de gestion du boîtier.

REMARQUE : Pour que des adresses DHCPv6 soient configurées avec succès, le paramètre **Enable IPv6** du boîtier doit être activé et un serveur DHCPv6 doit être configuré sur le réseau de gestion. Les cartes ILO et les modules d'interconnexion doivent être configurés séparément pour demander une adresse DHCPv6. S'ils sont configurés pour demander des adresses DHCPv6, les paramètres **Enable IPv6** et **Enable DHCPv6** doivent être activés pour autoriser le trafic nécessaire sur le réseau de gestion du boîtier.

REMARQUE : Après une réinitialisation usine, les paramètres de réseau IPv6 du boîtier (IPv6, SLAAC, DHCPv6 et annonces de routeur) sont activés par défaut.

REMARQUE : Lorsque les paramètres IPv6 Enable DHCPv6, Enable Router Advertisements ou Enable SLAAC enclosure sont désactivés sur le module Onboard Administrator, les adresses DHCPv6 ou SLAAC respectives des modules iLO du boîtier sont conservées jusqu'à leur expiration automatique en fonction de leur configuration respective. Une réinitialisation manuelle du module iLO libère immédiatement ces adresses.

Champ	Valeur possible	Description
IPv6 Static Address 1 (Adresse statique 1 IPv6)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1,2]	Adresse IPv6 1 de carte réseau externe du module Onboard Administrator.
IPv6 Static Address 2 (Adresse statique 2 IPv6)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1,2]	Adresse IPv6 2 de carte réseau externe du module Onboard Administrator.
IPv6 Static Address 3 (Adresse statique 3 IPv6)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1,2]	Adresse IPv6 3 de carte réseau externe du module Onboard Administrator.
IPv6 DNS Server 1 (Serveur DNS IPv6 1)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128. Le préfixe est facultatif.[1]	Adresse IPv6 du premier serveur DNS IPv6 statique.[3]

Champ	Valeur possible	Description
IPv6 DNS Server 2 (Serveur DNS IPv6 2)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128. Le préfixe est facultatif.[1]	Adresse IPv6 du deuxième serveur DNS IPv6 statique.[3]
Enable IPv6 Dynamic DNS (Activer DNS dynamique IPv6)	Activé (case cochée) ou désactivé (case non cochée).	Permet d'utiliser un nom d'hôte pour le module Onboard Administrator qui persiste même lorsque l'adresse IP attribuée de façon dynamique peut changer. Le nom d'hôte est inscrit avec un serveur DNS. Le DNS dynamique met à jour le serveur DNS avec des enregistrements nouveaux ou modifiés pour des adresses IP.[4] La désactivation de DNS dynamique sur le module Onboard Administrator arrête les mises à jour du module Onboard Administrator vers le serveur DNS. Toutefois, notez que certains serveurs DHCP peuvent disposer d'une clause pour mettre à jour des serveurs DNS directement. Pour désactiver totalement les mises à jour de DNS dynamique, désactivez le service DNS dynamique au niveau du module Onboard Administrator ainsi que sur le serveur DHCP.
Static Default Gateway (Passerelle statique par défaut)	####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. Ne spécifiez pas de préfixe. La passerelle est supposée être accessible au sein du réseau du module Onboard Administrator.[1]	Adresse IPv6 statique de la passerelle par défaut. Ce paramètre est requis dans un environnement de réseau IPv6 configuré pour être entièrement statique. Le module Onboard Administrator peut accepter une configuration de passerelle IPv6 directement via ce paramètre et, si configuré, via des annonces de routeur provenant de routeurs IPv6 sur le réseau de gestion. Si des annonces de routeur fournissent une configuration de passerelle IPv6, leur configuration de passerelle remplace le paramètre de passerelle IPv6 statique. La passerelle IPv6 en cours d'utilisation par le module Onboard Administrator est affichée dans le champ Current Default Gateway (Passerelle par défaut actuelle) sur l'écran Active Onboard Administrator TCP/IP Settings (Écran TCP/IP Settings du module Onboard Administrator actif à la page 211) et l'écran Standby Onboard Administrator TCP/IP Settings.
Static Route 1 (Route statique 1)	####:####:####:####:####:####:####:####/###, où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1]	Ajoute une route statique IPv6 à la table de routage du module Onboard Administrator (configuration manuelle).[5] La route statique définit un chemin d'accès explicite utilisé par

Champ	Valeur possible	Description
		le module Onboard Administrator pour accéder à un réseau externe via une passerelle. Dans une configuration réseau statique, la route statique supprime la nécessité de configurer le routeur pour envoyer des informations de route via des annonces de routeur. Si les annonces de routeur sont actives dans le réseau et que la passerelle par défaut est déjà configurée, le routeur informe tous les nœuds des routes statiques disponibles, ce qui rend ainsi la configuration manuelle des routes statiques inutile. Si vous spécifiez la route statique 1, vous devez également spécifier la passerelle associée (route statique 1).
Gateway (Static Route 1) (Passerelle [Route statique 1])	####:####:####:####:####:####:###:#### où #### est compris entre 0 et FFFF. Ne spécifiez pas de préfixe. La passerelle doit être accessible à la fois à partir du réseau du module Onboard Administrator et du réseau externe.[1]	Adresse IPv6 de la passerelle utilisant le chemin d'accès défini par la route statique 1. Vous devez également spécifier la route statique 1.
Static Route 2 (Route statique 2)	####:####:####:####:####:####:###:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1]	Ajoute une deuxième route statique IPv6 à la table de routage du module Onboard Administrator (configuration manuelle). Si vous spécifiez la route statique 2, vous devez également spécifier la passerelle associée (route statique 2).
Gateway (Static Route 2) (Passerelle [Route statique 2])	####:####:####:####:####:####:###:#### où #### est compris entre 0 et FFFF. Ne spécifiez pas de préfixe. La passerelle doit être accessible à la fois à partir du réseau du module Onboard Administrator et du réseau externe.[1]	Adresse IPv6 de la passerelle utilisant le chemin d'accès défini par la route statique 2. Vous devez également spécifier la route statique 2.
Static Route 3 (Route statique 3)	####:####:####:####:####:####:###:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1]	Ajoute une troisième route statique IPv6 à la table de routage du module Onboard Administrator (configuration manuelle). Si vous spécifiez la route statique 3, vous devez également spécifier la passerelle associée (route statique 3).
Gateway (Static Route 3) (Passerelle [Route statique 3])	####:####:####:####:####:####:###:#### où #### est compris entre 0 et FFFF. Ne spécifiez pas de préfixe. La passerelle doit être accessible à la fois à partir du réseau du module	Adresse IPv6 de la passerelle, utilisant le chemin d'accès défini par la route statique 3. Vous devez également spécifier la route statique 3.

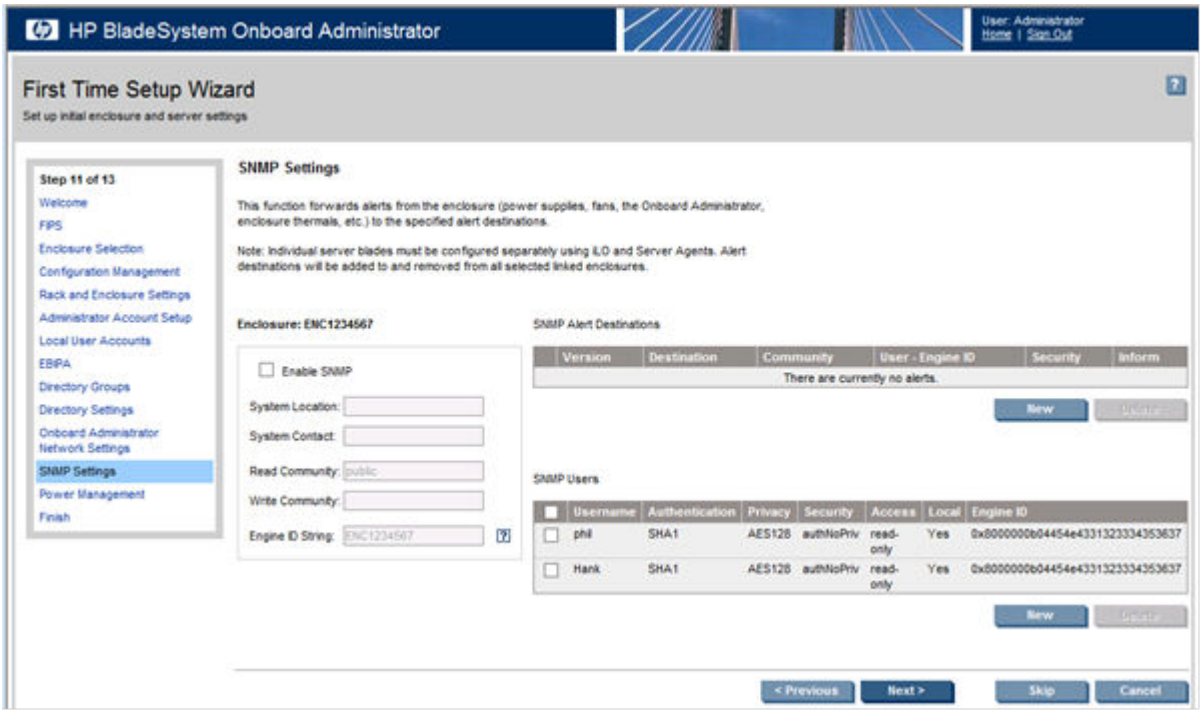
Champ	Valeur possible	Description
	Onboard Administrator et du réseau externe.[1]	

[1] Une version comprimée de la même adresse IPv6 est également prise en charge.
[2] Le module Onboard Administrator n'accepte pas une adresse locale de liaison comme adresse IPv6 statique.
[3] L'ordre dans lequel le module Onboard Administrator utilise des serveurs DNS est décrit dans l'onglet IPv6 Settings (Onglet IPv6 Settings à la page 129).
[4] Le système DNS dynamique IPv6 nécessite qu'un serveur DNS valide (IPv4 ou IPv6) soit configuré sur le module Onboard Administrator.
[5] **Attention** : L'ajout ou la suppression d'une route statique peut entraîner la perte de connectivité pour les clients qui accèdent au module Onboard Administrator.

Pour enregistrer les nouveaux paramètres IPv6, cliquez sur **Next** (Suivant).

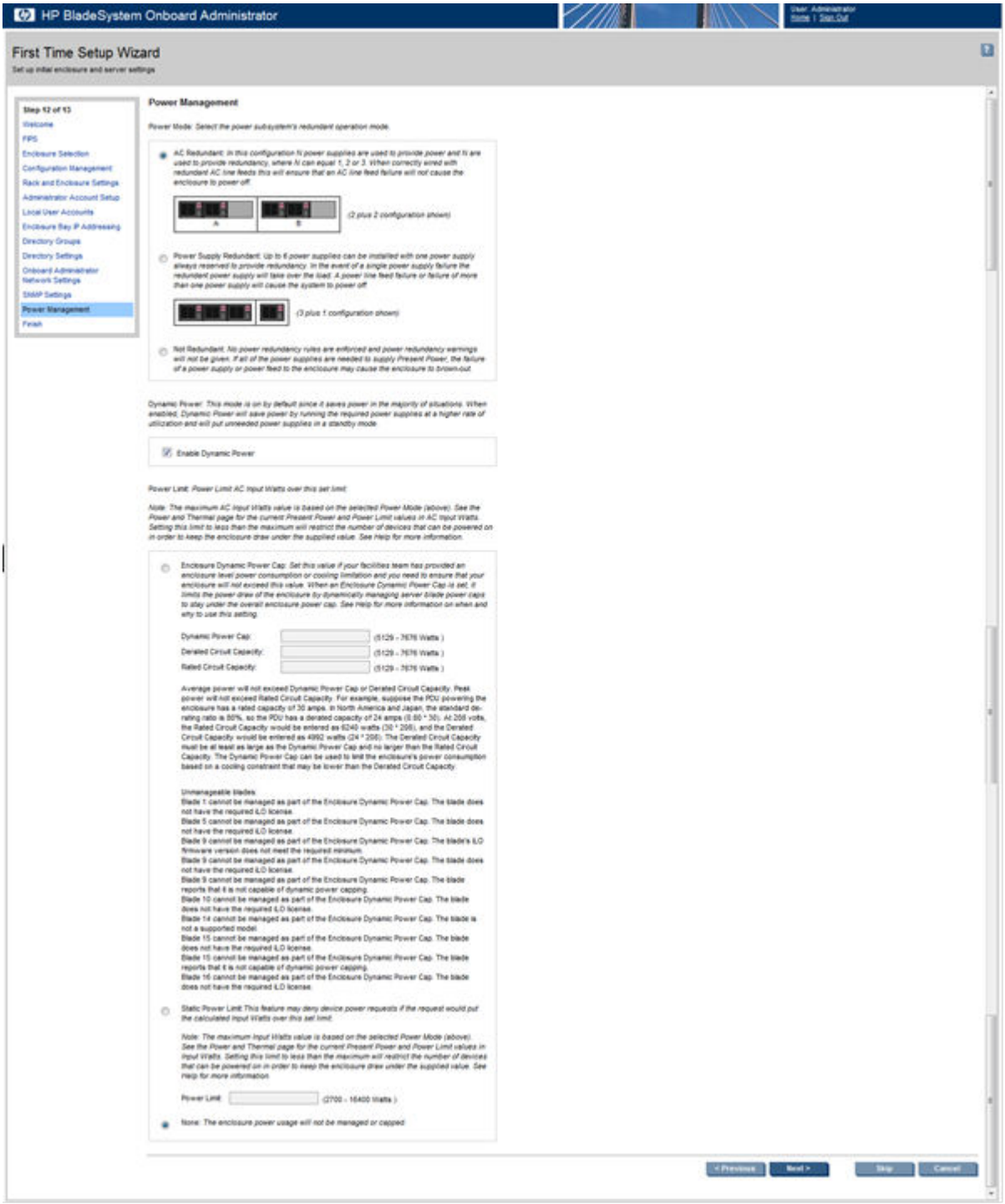
Écran Enclosure SNMP Settings

Utilisez l'écran Enclosure SNMP Settings (Paramètres SNMP du boîtier) pour configurer ou modifier les paramètres SNMP du HP BladeSystem Onboard Administrator actif.



Pour connaître les valeurs possibles et la description de chaque champ, consultez l'écran SNMP Settings (Paramètres SNMP) (Paramètres SNMP à la page 142).

Écran Power Management



REMARQUE : Si le mode de redondance est DC Redundant, AC Redundant ou Power Supply Redundant et que la redondance d'alimentation est perdue, vous devez ajouter des alimentations supplémentaires ou modifier le paramètre du mode de redondance dans le module Onboard Administrator pour restaurer l'état du sous-système d'alimentation. Consultez l'écran Insight Display pour connaître les mesures correctives.

REMARQUE : Pour modifier le mode de redondance d'alimentation, vous devez désactiver EDPC. Une fois le mode de redondance d'alimentation modifié, réinitialisez EDPC sur la base des nouvelles plages.

Options de gestion de l'alimentation

Le système de gestion d'alimentation du boîtier HP BladeSystem c3000 ou c7000 vous permet de configurer le boîtier selon vos besoins. Vous pouvez choisir parmi les options de gestion d'alimentation dans l'écran Onboard Administrator Power Management. Ces options de gestion d'alimentation sont décrites dans le tableau suivant.

Option de gestion de l'alimentation	Nom Insight Display	Description
Mode d'alimentation (mode de redondance d'alimentation)		
DC Redundant (redondance CC) ou AC Redundant (redondance CA)	DC Redundant (redondance CC) ou AC Redundant (redondance CA)	Le module OA détecte le type des blocs d'alimentation présents, adapte automatiquement le comportement du mode d'alimentation en conséquence et affiche le nom du mode correspondant : • Si des modules d'alimentation CC sont présents : mode de redondance CC • Si des modules d'alimentation CA sont présents : mode de redondance CA Également connu sous le nom redondance N+N ou redondance de grille. Les blocs d'alimentation *N* sont utilisés pour fournir l'alimentation et les blocs *N* sont utilisés pour fournir la redondance (où la valeur de *N* peut être 1, 2 ou 3). Jusqu'à trois alimentations peuvent s'avérer défectueuses sans entraîner de panne du boîtier. Lorsque le système est correctement câblé et comporte des lignes d'alimentation CC ou CA redondantes, cette configuration garantit que la panne d'une ligne d'alimentation CC ou CA n'entraîne pas la mise hors tension du boîtier. Au cas, peu probable, où la batterie de secours ne parvient pas à fournir l'alimentation en raison de plusieurs défaillances de bloc d'alimentation ou d'une panne du réseau électrique, le système peut être mis hors tension. Le système se met hors tension lorsque les blocs d'alimentation restants ne fournissent pas une alimentation suffisante pour répondre aux exigences d'alimentation du système. Les modes de redondance CA ou CC requièrent au moins deux

Option de gestion de l'alimentation	Nom Insight Display	Description
		blocs d'alimentation. Quel que soit le mode, HP recommande d'utiliser un nombre pair de blocs d'alimentation (2, 4 ou 6). Dans ce cas, *N* blocs d'alimentation servent à l'alimentation et *N* autres servent à assurer la redondance (où *N* est égal à 1, 2 ou 3). Si vous utilisez un nombre impair de blocs d'alimentation (3 ou 5), *N* sont utilisés pour fournir l'alimentation et N + 1 sont utilisés pour la redondance (où *N* est égal à 1 ou 2). Le mode de redondance CA ou CC protège également un système contre une panne du réseau électrique par l'utilisation d'un mode d'alimentation électrique de redondance CA ou CC (si correctement câblé). En mode de redondance CA, si vous utilisez un module d'entrée d'alimentation triphasée de boîtier c7000, HP recommande 6 blocs d'alimentation actifs (3+3) pour un équilibrage de phases correct.
Power Supply Redundant (Redondance d'alimentation)	Power Supply (Alimentation)	Pour tous les blocs d'alimentation. Ce mode prend en charge de deux à six blocs d'alimentation. Également appelé redondance N+1. Avec ce mode d'alimentation, *N* blocs d'alimentation servent à fournir l'alimentation et 1 est utilisé pour fournir la redondance (où la valeur *N* peut être 1, 2, 3, 4 ou 5). Si vous utilisez un module d'entrée d'alimentation triphasée de boîtier c7000, HP recommande 3 ou 6 blocs d'alimentation actifs (2+1 ou 5+1) pour un équilibrage de phases correct. Ce mode d'alimentation est conçu pour protéger le système en cas de panne de module d'alimentation. Dans le cas peu probable que plus d'un bloc d'alimentation ne parvient pas à fournir l'alimentation en raison de blocs d'alimentation défaillants ou d'une panne de grille d'alimentation, le système peut se mettre hors tension. Le système se met hors tension lorsque les blocs d'alimentation restants ne fournissent pas une alimentation suffisante pour répondre aux exigences d'alimentation du système.
Not Redundant (Non redondant)	Aucun	Pour tous les blocs d'alimentation. Ce mode prend en charge 1 à 6 blocs d'alimentation. Avec ce mode d'alimentation, *N* blocs d'alimentation servent à fournir l'alimentation et aucun

Option de gestion de l'alimentation	Nom Insight Display	Description
		n'est utilisé pour fournir la redondance (où la valeur *N* peut être 1, 2, 3, 4, 5 ou 6). Si vous utilisez un module d'entrée d'alimentation triphasée de boîtier c7000, HP recommande 3 ou 6 blocs d'alimentation actifs pour un équilibrage de phases correct Il n'existe pas de redondance d'alimentation et aucun avertissement de redondance d'alimentation n'est fourni. Si un bloc d'alimentation ne parvient pas à fournir l'alimentation en raison de blocs d'alimentation défaillants ou d'une panne de grille d'alimentation, le système peut se mettre hors tension. Il se mettra hors tension si les blocs d'alimentation restants ne disposent pas d'alimentation suffisante pour répondre aux exigences d'alimentation du système. Ce mode d'alimentation n'est pas recommandé pour les systèmes déployés dans des environnements de production.
Mode Alimentation dynamique (activé ou désactivé)		
Dynamic Power (Alimentation dynamique)	Dynamic Power (Alimentation dynamique)	S'il est activé, le mode d'alimentation dynamique place les alimentations inutilisées en mode Standby afin d'accroître l'efficacité de l'alimentation du boîtier et de réduire la consommation électrique du boîtier pendant les demandes plus faibles d'alimentation. L'augmentation de la demande en alimentation entraîne automatiquement le passage en mode pleinement opérationnel des alimentations en attente. Ce tableau est suivi d'informations supplémentaires sur l'alimentation dynamique.
Mode Limite de puissance		
Enclosure Dynamic Power Cap (Limitation dynamique de la puissance du boîtier)	Aucun	Permet de spécifier une limite pour la consommation électrique du boîtier. Le tirage de puissance est limité par la gestion dynamique des limitations d'alimentation des lames de serveur afin de rester sous la limitation d'alimentation globale du boîtier. Pour plus d'informations, consultez le tableau de limite de puissance qui suit.
Static Power Limit (Limite de puissance statique)	Power Limit (Limite de puissance)	Paramètre facultatif de limitation de la puissance. Chaque fois que vous essayez de mettre sous tension un périphérique, les demandes de puissance totale du nouveau périphérique et des périphériques déjà sous tension sont comparées à cette limite de puissance statique. Si les

Option de gestion de l'alimentation	Nom Insight Display	Description
		demandes de puissance totale dépassent la limite, la mise sous tension du nouveau périphérique est refusée. Pour plus d'informations sur la limite de puissance statique et la manière dont elle est comparée au plafond d'alimentation dynamique de boîtier, consultez le tableau de limite d'alimentation qui suit.

REMARQUE : Quel que soit le mode de redondance activé, tous les blocs d'alimentation fonctionnels présents dans le boîtier sont généralement actifs et partagent la prestation des besoins en alimentation du boîtier. Si le mode Alimentation dynamique est activé, certains blocs d'alimentation peuvent être placés automatiquement en veille pour augmenter l'efficacité globale de l'alimentation du boîtier. Pour plus d'informations, consultez la discussion relative au mode Alimentation dynamique qui suit.

Le module Onboard Administrator permet de modifier le paramètre de mode d'alimentation (redondance) après la mise sous tension du boîtier et des périphériques. Si le mode d'alimentation est modifié, le module Onboard Administrator actualise l'état de redondance en fonction des besoins, en signalant une redondance dégradée/défectueuse le cas échéant. Par exemple, le mode d'alimentation d'origine était Alimentation redondante (N+1) lorsque toutes les lames ont été mises sous tension, puis a été modifié sur Redondant CA (N+N), réduisant ainsi la capacité de puissance telle que vue par le module Onboard Administrator. Tant qu'une puissance suffisante est disponible, toutes les lames resteront opérationnelles. Toutefois, dans certaines circonstances, une lame ne se mettra pas sous tension, par exemple lorsque qu'elle remplace une autre lame de serveur. Des informations supplémentaires sont fournies dans le tableau et les sections qui suivent.

Dynamic Power (Alimentation dynamique) : le paramètre par défaut est Disabled (Désactivé). Les sélections suivantes sont valides :

- Enabled (Activé) : certaines alimentations peuvent être automatiquement placées en veille pour augmenter l'efficacité globale du sous-système d'alimentation du boîtier.
- Disabled (Désactivé) : toutes les alimentations partagent la charge. L'efficacité du sous-système d'alimentation varie en fonction de la charge.

REMARQUE : L'alimentation dynamique est prise en charge avec tous les blocs d'alimentation c3000. Elle est prise en charge avec tous les blocs d'alimentation c7000, à l'exception de ceux fonctionnant avec une tension d'entrée basse (nominale 100-120 VCA).

REMARQUE : Pour OA v4.01 et versions ultérieures, la valeur usine par défaut associée au paramètre Dynamic Power a été modifiée d'activée à désactivée. L'efficacité de fonctionnement des blocs d'alimentation de boîtiers HP Gold (rendement de 92 %) et HP Platinum (rendement de 94 %) actuellement disponible rend inutile cette stratégie de gestion de l'alimentation basée sur le microprogramme. Le paramètre Dynamic Power est recommandé uniquement pour les blocs d'alimentation de boîtier HP ayant une valeur de rendement inférieure à 92 %. Lors de la mise à niveau à OA v4.01 ou version ultérieure, le paramètre Dynamic Power actuel est conservé après la mise à niveau. Pour plus d'informations, consultez l'avis à la clientèle c03957955 (http://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03957955).

Power Limit (Limite de puissance)

Ne définissez pas de limite de puissance statique ou de plafond d'alimentation dynamique de boîtier sur un boîtier vide.

Mode	Nom Insight Display	Description
Enclosure Dynamic Power Cap (Limitation dynamique de la puissance du boîtier)	Aucun	Une fonctionnalité facultative qui permet de limiter les serveurs dans un boîtier en tant que groupe. Lorsque les serveurs fonctionnent, la demande en puissance varie en fonction de chaque serveur. Un plafond d'alimentation est configuré pour chaque serveur de manière à ce qu'il dispose de suffisamment de puissance pour répondre aux exigences de sa charge de travail tout en tenant compte du plafond d'alimentation dynamique du boîtier. Une carte OA redondante est requise pour paramétrer la fonction Dynamic Power Cap (Plafond d'alimentation dynamique). La fonction est activée avec trois paramètres de configuration : • Dynamic Power Cap (Plafond d'alimentation dynamique) : la consommation électrique moyenne totale du boîtier ne dépassera pas le plafond d'alimentation dynamique. • Derated Circuit Capacity (Capacité réduite du circuit) : la consommation électrique moyenne sur un circuit unique ne dépassera pas la capacité réduite du circuit. • Rated Circuit Capacity (Capacité nominale du circuit) : la consommation électrique de pointe sur un circuit unique ne dépassera pas la capacité nominale du circuit. Lors de la configuration de ces paramètres, le déclassement de puissance du circuit doit être au moins aussi élevé que le plafond de puissance dynamique et non supérieur à la capacité nominale du circuit. Le plafond d'alimentation dynamique est utilisé pour limiter la consommation électrique du boîtier sur la base d'une contrainte de refroidissement qui peut être inférieure à la capacité réduite du circuit. La capacité réduite du circuit est utilisée pour limiter la consommation électrique moyenne du boîtier sur un circuit. La capacité nominale du circuit est utilisée pour limiter la

Mode	Nom Insight Display	Description
		consommation électrique de pointe du boîtier sur un circuit. Si vous devez limiter la charge électrique ou la sortie thermique d'un boîtier, la méthode de plafond d'alimentation dynamique du boîtier est meilleure qu'une limite d'alimentation statique. Enclosure Dynamic Power Cap permet d'alimenter plus de lames que sur une limite d'alimentation statique.
Static Power Limit (Limite de puissance statique)	Power Limit (Limite de puissance)	Paramètre facultatif de limitation de la puissance. Chaque fois que vous essayez de mettre sous tension un périphérique, les demandes de puissance totale du nouveau périphérique et des périphériques déjà sous tension sont comparées à cette limite de puissance statique. Si les demandes de puissance totale dépassent la limite, la mise sous tension du nouveau périphérique est refusée. Une limite d'alimentation statique est meilleure lorsque : • Vous ne souhaitez imposer à vos lames des plafonds ajustés de manière dynamique. • Vous préférez ne pas alimenter une lame de serveur s'il est impossible de lui attribuer la pleine puissance (même si elle consomme typiquement moins). • Plus d'1/4 des lames du boîtier ne satisfont pas aux exigences définies pour le matériel ou le microprogramme eu égard au plafond d'alimentation dynamique du boîtier.
Aucun	Aucun	La consommation d'énergie du boîtier n'est pas supervisée ou plafonnée.

Différences entre plafond d'alimentation, plafond d'alimentation dynamique et plafond d'alimentation dynamique du boîtier

HP offre trois variétés de gestion de l'alimentation qui permettent aux utilisateurs de limiter la consommation d'énergie du serveur. Les trois variétés de plafonnement de l'alimentation fonctionnent pour limiter la consommation suivant un objectif en watts ou Btu/hr spécifié. Les trois technologies sont Plafond d'alimentation, Plafond d'alimentation dynamique et Plafond d'alimentation dynamique du boîtier.

Plafond d'alimentation

En mai 2007, HP a lancé la technologie de plafond d'alimentation avec la version 1.30 d'iLO 2. Cette technologie basée sur le microprogramme limite la consommation moyenne du serveur à une valeur

en watts ou Btu/hr définie par l'utilisateur. Dans la mesure où cette technologie fonctionne dans le microprogramme, elle ne peut pas limiter la consommation d'alimentation assez rapidement pour assurer la protection des disjoncteurs au niveau des unités PDU. Le plafond d'alimentation limitant la consommation électrique assez rapidement pour protéger l'infrastructure de refroidissement, ceci est donc une solution efficace pour les centres de données faisant face à des contraintes de capacité de refroidissement. Le plafond d'alimentation est pris en charge sur tout serveur ou lame ProLiant doté d'un processeur de supervision iLO et de possibilités de mesure de puissance. L'utilisation du plafond d'alimentation requiert un microprogramme iLO 2 version 1.30 (ou ultérieure) et d'une paire ROM/BIOS système mise à jour.

Plafond dynamique de puissance

Le plafond dynamique de puissance est une technologie basée sur le matériel qui limite la consommation de puissance suffisamment rapidement pour protéger les disjoncteurs et l'infrastructure de refroidissement. En décembre 2008, HP a lancé la technologie de plafond dynamique d'alimentation avec la version 1.70 d'iLO 2. Les serveurs pris en charge contiennent un circuit matériel interne qui surveille la consommation d'énergie du serveur sur une base sous-secondaire. Si la consommation d'énergie du serveur s'approche de la limite de plafond d'alimentation définie dans iLO, le circuit matériel interne limite la consommation électrique suffisamment rapidement pour protéger les circuits au niveau de l'unité PDU d'un dépassement de souscription et empêcher les pannes de serveur liées à l'alimentation.

Le plafond dynamique d'alimentation requiert un matériel spécifique sur la carte mère. Le plafond dynamique d'alimentation requiert également le microprogramme iLO 2 version 1.70 (ou ultérieure) et un système ROM/BIOS daté du 01/10/2008 (ou ultérieur). iLO met automatiquement à jour le microprogramme dans le circuit matériel d'alimentation du plafond d'alimentation dynamique.

La limitation dynamique de la puissance du boîtier est prise en charge sur les lames de serveur BladeSystem suivantes :

- BL260c G5 (Remarques : 2)
- BL2x220 G5 (Remarques : 2)
- BL460c G1 (Remarques : 1 et 2)
- BL460c G5 (Remarques : 2)
- BL465c G5 (Remarques : 2)
- BL495c G5 (Remarques : 2)
- BL685c G5 (Remarques : 2)
- Toutes les lames de serveur G6
- Toutes les lames de serveur G7
- Toutes les lames de serveur G8

Informations complémentaires

- Ces systèmes nécessitent des cartes mère compatibles Quatre cœurs pour prendre en charge la limitation dynamique de la puissance.
- Lors de la mise en œuvre de la limitation de puissance pour HP BladeSystem, HP recommande d'utiliser la limitation dynamique de la puissance de boîtier définie dans l'ensemble du module Onboard Administrator. Pour utiliser la limitation dynamique de la puissance de boîtier, vous devez mettre à niveau le microprogramme iLO 2 à la version 1.70 ou ultérieure et vous êtes encouragé à mettre à jour la ROM système à la version 10/1/2008 ou ultérieure. Pour certains serveurs BL460c plus anciens, le microprogramme iLO peut ne pas pouvoir mettre à jour automatiquement le circuit matériel de limitation dynamique de la puissance. Dans ce cas, le

module Onboard Administrator compense l'absence du circuit matériel interne et continue de garantir la protection du circuit.

Plafond d'alimentation dynamique du boîtier

Enclosure Dynamic Power Capping combine la technologie de plafond dynamique d'alimentation du serveur BladeSystem avec un algorithme de contrôle d'équilibrage de l'alimentation dans le module Onboard Administrator afin de maximiser le rendement global du boîtier. Enclosure Dynamic Power Capping protège vos disjoncteurs et maximise votre rendement.

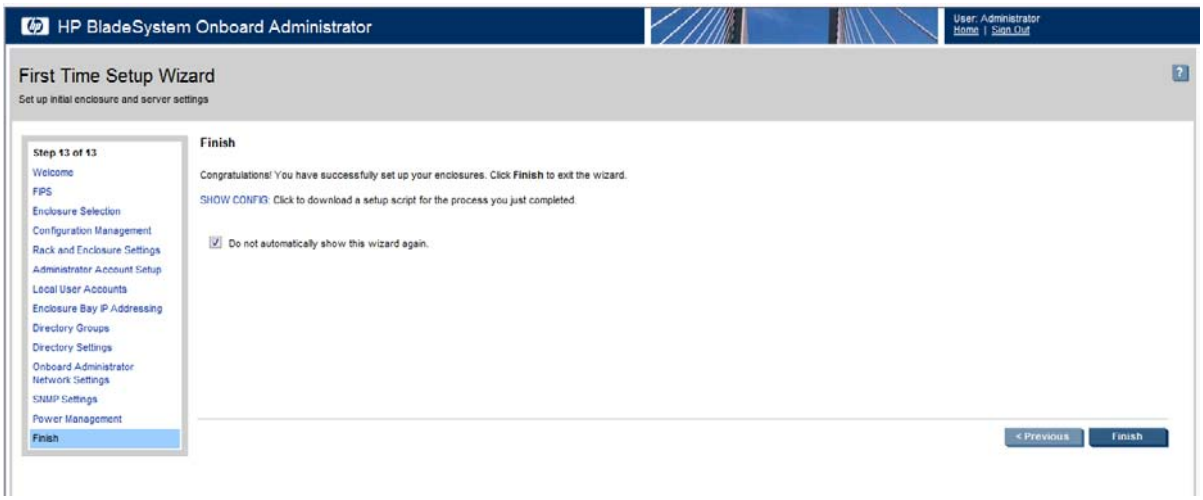
À l'aide du plafond d'alimentation dynamique du boîtier, vous définissez un plafond d'alimentation pour l'ensemble du boîtier. Le module Onboard Administrator alloue des limites individuelles à chaque lame de serveur participante. Les lames de serveur gèrent leur consommation suivant cette limite. Le module Onboard Administrator surveille continuellement les exigences de consommation pour chaque lame de serveur et rééquilibre en permanence les limites individuelles afin de veiller à ce que les lames de serveur occupées reçoivent plus de puissance que les lames de serveur inactives. Cette allocation d'alimentation améliore les performances globales du boîtier.

Les plafonds d'alimentation de serveur BladeSystem sont définis dans le module Onboard Administrator. Enclosure Dynamic Power Capping protège les infrastructures électriques et de refroidissement. Enclosure Dynamic Power Capping fonctionne avec la technologie de plafonnement de l'alimentation basée sur le microprogramme sur le serveur ou avec la technologie rapide, basée sur le matériel. La solution Enclosure Dynamic Power Capping fonctionne mieux si les lames de serveur qui prennent en charge la technologie rapide de plafonnement basée sur le matériel sont mises à jour.

Enclosure Dynamic Power Capping requiert Onboard Administrator 2.30 (ou ultérieure), iLO 2 version 1.70 (ou ultérieure) et une paire ROM/BIOS système datée du 01/10/2008 (ou d'une date ultérieure).

REMARQUE : Les plafonds d'alimentation définis pour moins de 50 % de la différence entre la puissance maximale et la puissance au ralenti peuvent devenir inaccessibles en raison de changements dans le serveur. Les plafonds d'alimentation définis pour moins de 20 % ne sont pas recommandés, et peuvent engendrer un redémarrage du serveur ou un arrêt de la réponse du système d'exploitation du serveur.

Finalisation



Pour télécharger une configuration actuelle pour le boîtier :

1. Cliquez sur le lien **SHOW CONFIG** (Afficher la configuration). La configuration s'ouvre dans une nouvelle fenêtre de navigateur.
2. Pour enregistrer la configuration en tant que fichier texte, choisissez une des options suivantes :
   - Si vous utilisez Microsoft Internet Explorer, sélectionnez **Save As** (Enregistrer sous).
   - Si vous utilisez Mozilla Firefox, sélectionnez **Save Page As** (Enregistrer la page sous).
   - Si vous utilisez Google Chrome, sélectionnez **Save Link As** (Enregistrer la link sous).

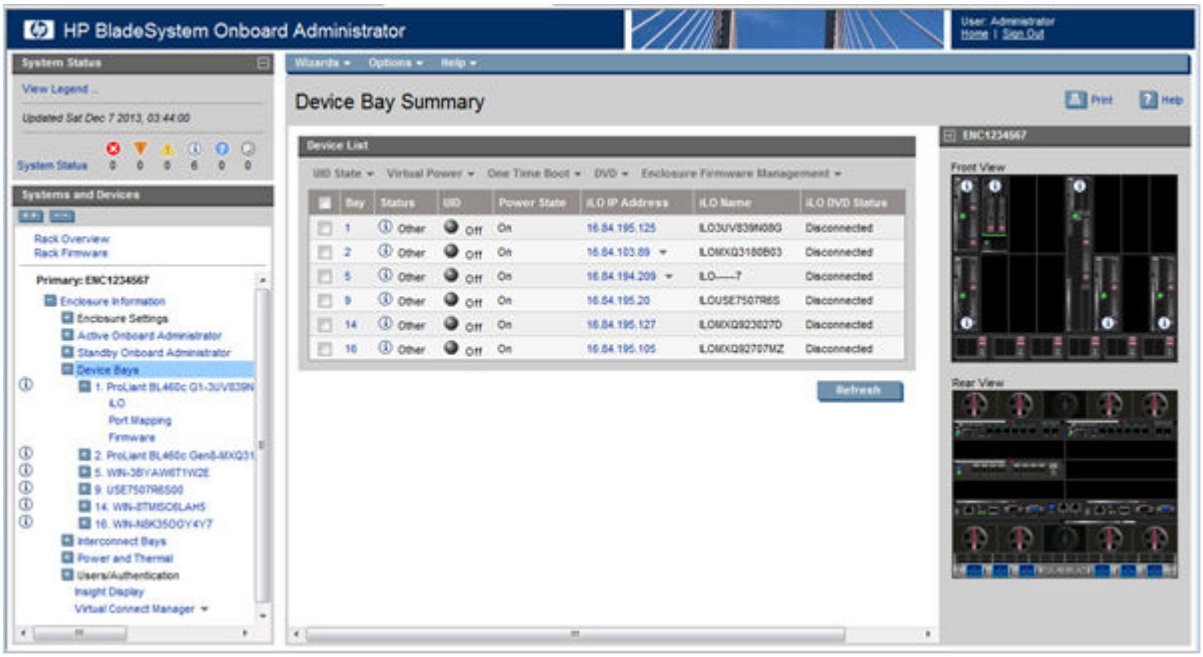
Pour des raisons de sécurité, la configuration actuelle récupérée ne contient pas de mot de passe utilisateur. Vous pouvez modifier manuellement le script pour ajouter les mots de passe utilisateur après le nom d'utilisateur sur les lignes ADD USER. En outre, la configuration actuelle récupérée ne contient pas de paramètres LCD (Lock Buttons [Boutons de verrouillage], Enable PIN Protection [Activer la protection PIN] et PIN Code [Code PIN]). Ces paramètres ne peuvent pas être ajoutés à partir du script de configuration.

Pour forcer le redémarrage de l'assistant de première installation lors de la prochaine connexion d'un utilisateur au module Onboard Administrator, vous pouvez désactiver la case **Do not automatically start this wizard again** (Ne pas redémarrer automatiquement cet assistant).

Pour enregistrer les paramètres et quitter l'assistant First Time Setup, cliquez sur **Finish** (Terminer). L'écran de l'assistant se ferme et vous revenez à l'écran principal par défaut du module HP BladeSystem Onboard Administrator.

6 Navigation dans le module Onboard Administrator

Présentation de la navigation

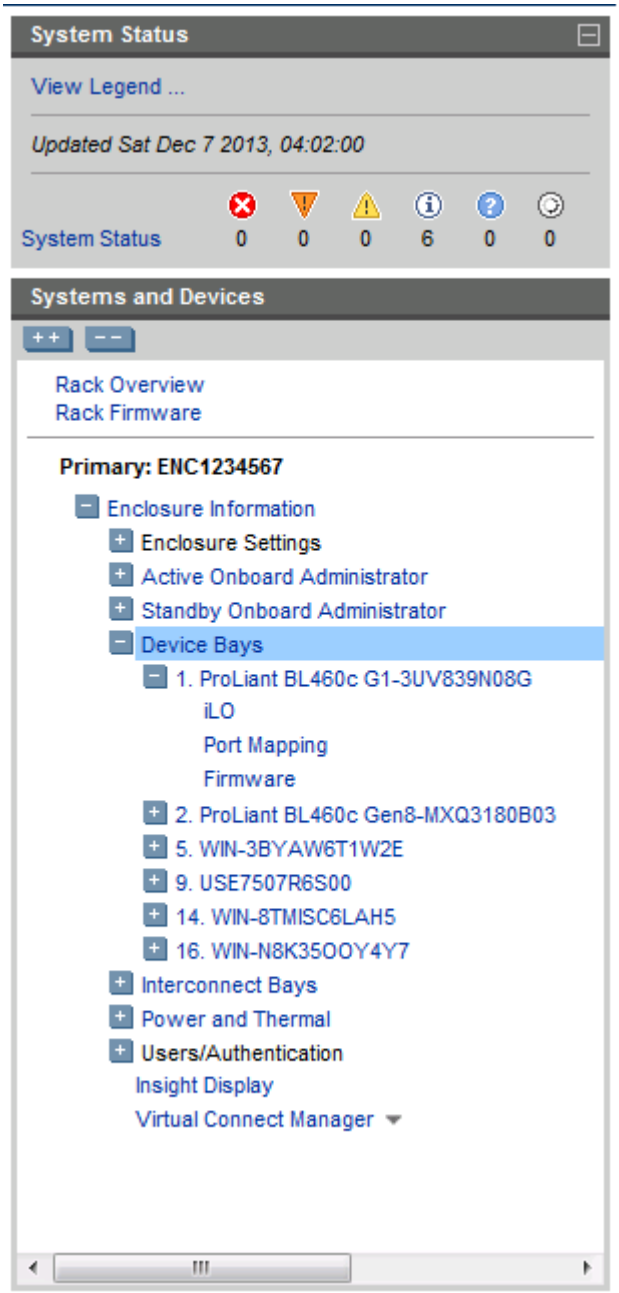


Le système de navigation principal de HP BladeSystem Onboard Administrator se compose d'une arborescence située sur le côté gauche de l'écran, qui facilite la navigation à travers les différents écrans de l'interface graphique. Il reste visible lors de la navigation dans l'arborescence. Le centre de l'écran affiche des informations d'état et des paramètres que vous pouvez modifier. Le côté droit de l'écran affiche une image physique du boîtier. Vous pouvez naviguer à travers les périphériques du boîtier et les fonctions en utilisant l'arborescence ou la vue graphique.

Arborescence

L'arborescence facilite la navigation hiérarchique au sein des périphériques et fonctions de différents boîtiers. L'affichage de l'arborescence dépend de plusieurs facteurs tels que les autorisations utilisateur, la disponibilité d'un périphérique ou son état. Ainsi, un utilisateur configuré en tant qu'opérateur ou utilisateur ne verra pas certaines options dans l'arborescence.

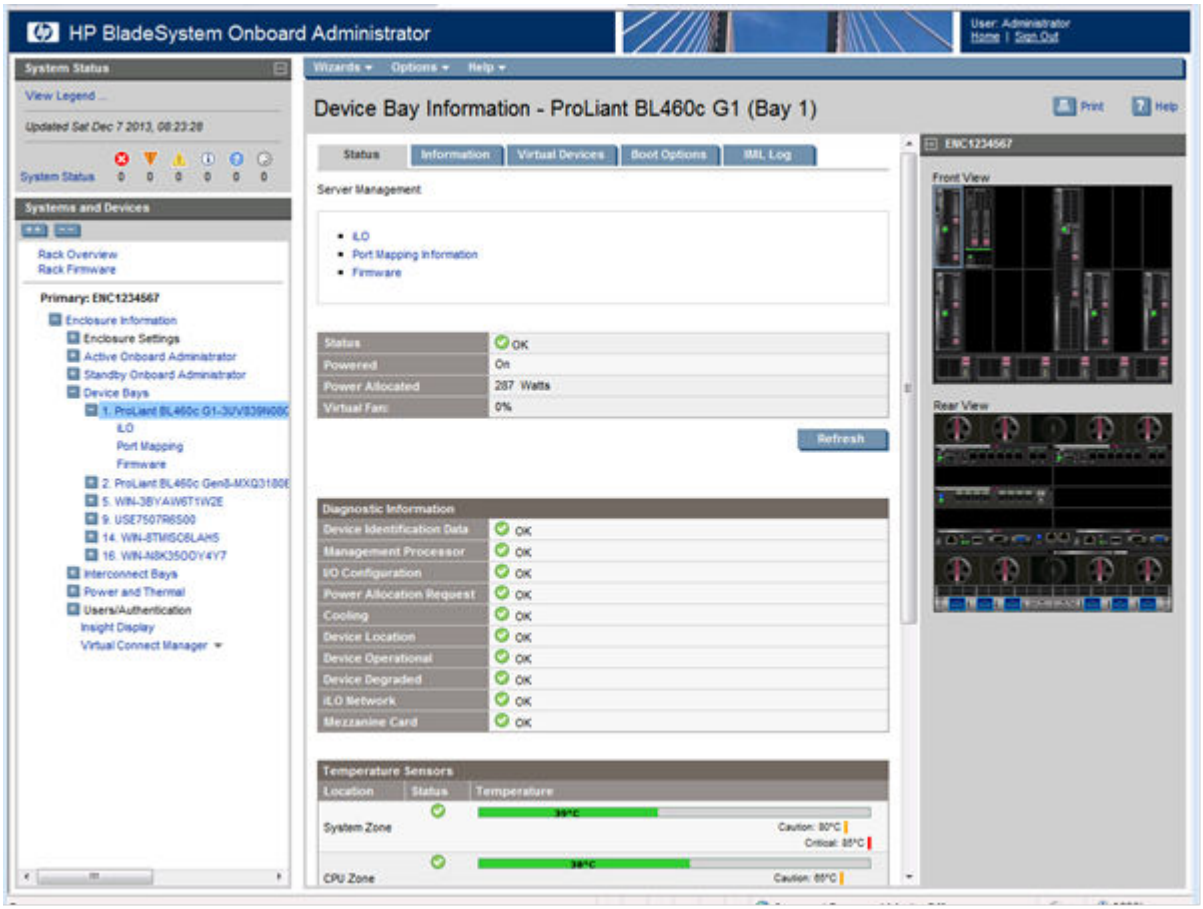
Les trois vues sont similaires pour les boîtiers c3000 et c7000.



La vue d'arborescence permet de naviguer à l'aide de catégories basées sur les principaux systèmes inclus dans le boîtier. Lorsqu'une catégorie est développée en cliquant sur le signe à gauche de la catégorie, une icône en regard du nom de la catégorie peut indiquer l'état détérioré du système concerné. En cas d'état regroupant plusieurs composants, l'icône d'état indique le plus mauvais état cumulé de tous les périphériques de la même catégorie.

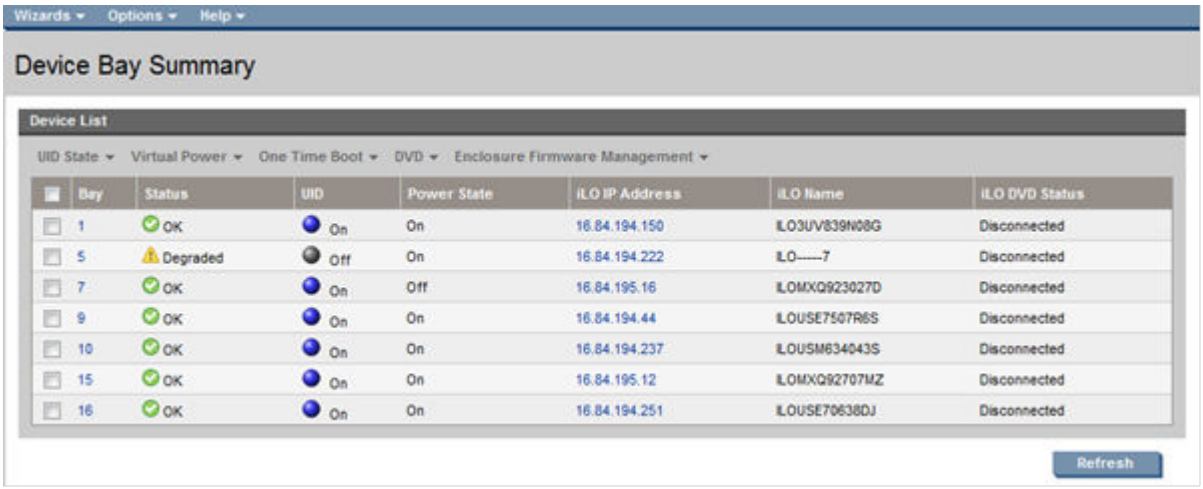
Pages de chaque périphérique

Lorsque vous cliquez sur le lien d'un périphérique individuel, le périphérique est sélectionné, sa page de détails s'ouvre et le périphérique est sélectionné dans la vue graphique dans la partie droite de l'écran. Les pages de chaque périphérique contiennent des informations détaillées sur le périphérique sélectionné et sur d'autres fonctions liées à ce périphérique.



Pages de résumé des catégories

Les pages de résumé des catégories comportent des informations sur chacun des périphériques répertoriés sous chaque catégorie. Ainsi, si vous cliquez sur le lien **Device Bays** (Baies de périphérique), la page de résumé d'une baie s'ouvre. Chaque élément parent de l'arborescence fonctionne comme suit. Lorsque vous cliquez sur un lien de résumé de catégorie, aucun périphérique n'est sélectionné dans la navigation de la vue graphique.



Pages de formulaire système

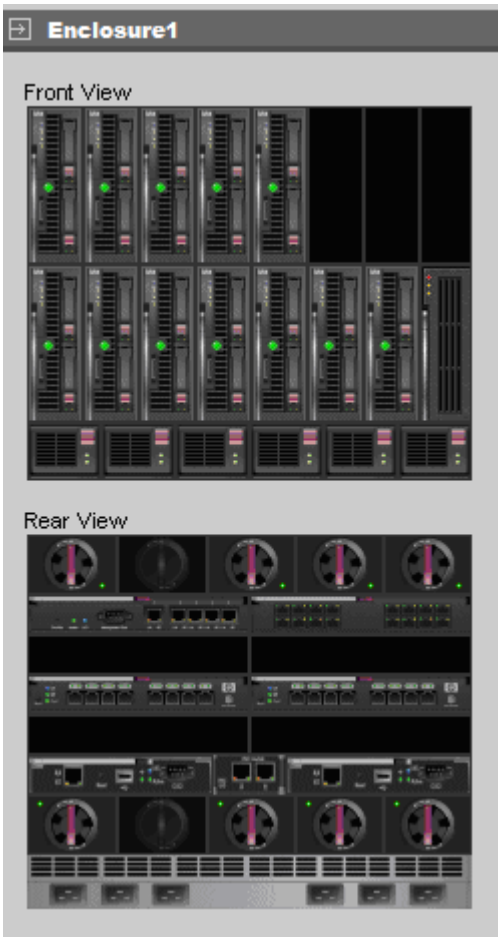
Certains périphériques, et en particulier le module HP Onboard Administrator, peuvent avoir des liens vers différentes pages de formulaires système répertoriés sous leur lien principal dans l'arborescence

à gauche. Les pages de formulaire contiennent des zones de saisie de texte, des cases d'option ainsi que d'autres éléments HTML de saisie. Ces pages servent à administrer les paramètres liés au périphérique auquel elles appartiennent. Ainsi, vous pouvez utiliser la page de formulaire du système HP Onboard Administrator pour modifier les paramètres d'adresse IP et mettre à jour le microprogramme. Ces formulaires sont tous liés sous l'élément parent du module HP Onboard Administrator. Lorsque vous cliquez sur un lien de formulaire du système, le périphérique auquel appartient la page de formulaire est sélectionné dans la vue graphique. Si vous cliquez par exemple sur le lien **Firmware Update** (Mise à jour du microprogramme) du module HP Onboard Administrator actif, le système sélectionne le périphérique du HP Onboard Administrator actif dans la vue graphique. Les liens vers les formulaires système n'affichent pas d'icône d'état.

Navigation dans la vue graphique

Le deuxième élément du système de navigation de l'interface du HP BladeSystem Onboard Administrator est la représentation graphique du boîtier physique, appelée vue graphique. La vue graphique consiste en deux sous-composants : une vue avant et une vue arrière.

L'image suivante illustre la vue graphique d'un boîtier c7000 typique.



L'image suivante illustre la vue graphique d'un boîtier c3000 typique.

Toutes les fonctions et fonctionnalités de la navigation dans la vue graphique sont les mêmes pour les boîtiers c3000 et c7000, sauf quelques exceptions mentionnées.

Sélection d'un périphérique

Pour sélectionner un périphérique, cliquez sur sa représentation graphique dans la vue graphique avant ou arrière. Lorsque vous sélectionnez un périphérique, la bordure qui l'entoure passe du gris au bleu clair pour indiquer qu'il s'agit du périphérique actuellement sélectionné. La sélection d'un périphérique en vue graphique entraîne la sélection du périphérique correspondant dans la vue de l'arborescence de navigation à gauche. Chaque fois que vous sélectionnez un périphérique à partir d'une zone du système de navigation, le reste de la navigation reflète cet événement de sélection de périphérique et se met à jour en conséquence.

Signalement des états

La vue graphique indique l'état de chaque périphérique présent dans le boîtier. Cet état est indiqué par une petite icône sur le périphérique. Aucune icône ne s'affiche pour un périphérique qui fonctionne correctement et dont l'état est normal (OK). Toutefois, tous les autres codes d'état s'affichent sous forme d'icônes sur le périphérique.

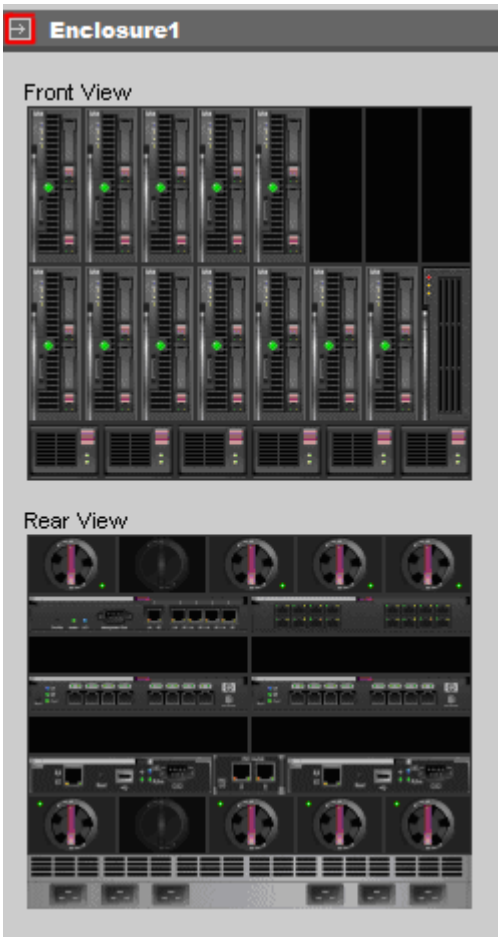
La vue graphique n'indique pas la présence ou l'absence de disques durs dans la lame de serveur ou la lame de stockage.

Sécurité du périphérique

Bien que les autorisations utilisateur aient une incidence sur les vues graphiques avant et arrière, la sécurité de la vue graphique n'est pas traitée de la même façon que dans la vue de l'arborescence à gauche. Si l'utilisateur n'est pas autorisé à accéder à un périphérique, une baie vide s'affiche, que cette baie comporte ou non un périphérique. Une icône en forme de cadenas s'affiche également dans la cellule du tableau de la baie pour indiquer que celle-ci est verrouillée pour l'utilisateur courant.

Réduction de la vue graphique

Pour réduire la vue graphique à partir de l'écran principal, cliquez sur la petite case contenant une flèche et située directement à gauche du nom du boîtier dans la zone de la vue graphique. Vous réduisez ainsi la vue graphique et laissez plus de place à l'affichage de la section principale. Cette réduction est utile lorsque vous visualisez le module Onboard Administrator sur un petit écran ou sur des écrans basse résolution.



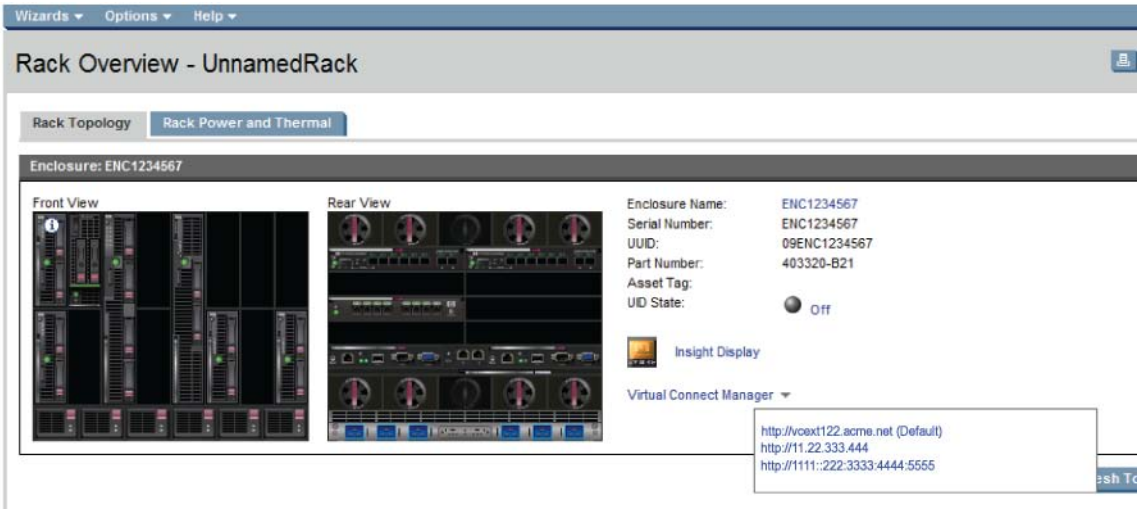
7 Vue du rack

Écran Rack Overview

L'onglet Rack Topology (Topologie du rack) fournit une représentation graphique du boîtier physique que l'on appelle vue graphique. La vue graphique consiste en une vue avant et une vue arrière. Lorsque vous déplacez la souris au-dessus d'un périphérique dans la vue graphique, une fenêtre s'ouvre et affiche les informations relatives à ce périphérique. La vue graphique fournit l'état de chaque périphérique au sein du boîtier et donne la possibilité de sélectionner chacun pour obtenir des informations plus détaillées.

S'il existe plusieurs boîtiers, certains d'entre eux peuvent s'afficher en gris dans l'écran Rack Overview (Présentation du rack). Pour afficher le contenu et les informations de ces boîtiers, entrez un nom d'utilisateur et un mot de passe dans les zones de texte, puis cliquez sur **Sign In** (Connexion). Une vue graphique du boîtier s'affiche. Le schéma suivant illustre la présentation du rack avec un boîtier grisé.

Après vous être inscrit, le contenu du boîtier devient disponible, comme indiqué dans l'exemple suivant. Pour se connecter à une instance de VCM, cliquez sur le bouton fléché vers le bas en regard de « Virtual Connect Manager ». Une fenêtre contextuelle affiche les liens d'adresse Web que vous pouvez utiliser pour une connexion à une instance de VCM. Si la prise en charge du lien FQDN est activée et que certaines exigences de configuration DNS sont remplies, une adresse Web VCM basée sur FQDN est la sélection par défaut, comme indiqué. Pour plus d'informations sur l'activation de la prise en charge du lien FQDN, consultez la page « Accès réseau ».



Informations sur le rack

Rangée	Description
Enclosure name (Nom du boîtier)	Nom configuré par l'utilisateur du boîtier dans le rack.
Enclosure Rack U Position (Position U du rack du boîtier)	Emplacement du boîtier dans le rack.
Serial Number (Numéro de série)	Numéro de série unique du boîtier.
UUID	Identifiant universel unique affecté au boîtier.
Part Number (Référence)	Référence du boîtier utilisée lors de l'obtention d'un nouveau boîtier ou d'un boîtier de remplacement.
Asset Tag (Étiquette d'inventaire)	L'étiquette d'inventaire est utilisée à des fins de contrôle des stocks.
UID State (État UID)	Affiche On ou Off selon que l'UID est actif ou non.

Informations sur l'emplacement du rack

Rangée	Description
Rack Name (Nom du rack)	Le nom du rack.
Rack Product Description (Description du produit du rack)	Nom descriptif commun du rack.
Rack Part Number (Référence du rack)	Référence à utiliser pour commander un rack de remplacement.
Rack Identifier (Identificateur du rack)	Chaîne unique qui identifie le rack.
Rack U Height (Hauteur U du rack)	Hauteur U du rack.

Utilisation de la fonction Location Discovery Services

La fonction Location Discovery Services est un composant de HP Discovery Services. La fonction Location Discovery Services signale automatiquement les emplacements de serveur à HP SIM et Insight Control, en éliminant cette tâche manuelle pour les administrateurs de serveurs. Les administrateurs peuvent utiliser les informations de localisation et les données système avec HP Asset Manager pour obtenir des données d'actifs plus précises et complètes.

La technologie Location Discovery Services est une solution de détection d'emplacements U de rack pour les racks G3 et de versions ultérieures. Elle permet au microprogramme de châssis SL, HP iLO et Onboard Administrator de serveur BL de signaler et d'afficher l'identifiant de rack et la position U du serveur dans le rack. Les racks pris en charge sont programmés avec des valeurs U uniques en modules 7U et/ou 8U, et sont installés avec le numéro de version d'étiquette, l'identifiant de rack, le numéro de référence, le nom du produit, la hauteur de rack, ainsi que la position U. La solution Location Discovery Services prend en charge les racks 14U, 22U, 36U, 42U et 47U.

Le périphérique de rack lit l'étiquette d'emplacement U du rack chaque fois que iLO reçoit une alimentation secteur ou que iLO est réinitialisé. La valeur de position U indique la position U lue par le périphérique. Le décalage de la position de contact est une valeur fixe pour chaque modèle qui indique la position du contact par rapport à la position U inférieure du périphérique. Il est normalement de 0, mais peut être une valeur positive si le contact ne peut pas être placé à la position U inférieure du périphérique. La position U la plus basse occupée par le périphérique est calculée en soustrayant le décalage U de la position U.

Vous pouvez afficher les données détectées dans certains écrans Onboard Administrator, tels que le tableau des informations sur le rack dans l'onglet Enclosure Information. En outre, plusieurs commandes de l'interface CLI Onboard Administrator affichent les données détectées, par exemple les commandes `SHOW ENCLOSURE INFO` et `SHOW TOPOLOGY INFO`. Pour plus d'informations sur ces commandes, reportez-vous au *Manuel de l'utilisateur de l'interface de ligne de commande HP BladeSystem Onboard Administrator*.

Rack Information	
Enclosure Rack U Position	21
Rack Product Description	HP 42U Intelligent Series Rack
Rack Part Number	BW946A
Rack Identifier	CN82190004
Rack U Height	42

Modes de topologie

Le module Onboard Administrator prend en charge trois modes de topologie qui sont déterminés par la sélection effectuée sur l'écran de connexion préalable à la connexion. Les trois modes de topologie sont les suivants :

- Mode local : utilisé pour superviser un boîtier unique lorsque plusieurs boîtiers peuvent être sélectionnés. Le module Onboard Administrator ignore toutes les modifications de topologie. Ce mode est utile lorsque vous ne souhaitez pas modifier la topologie en ajoutant des boîtiers liés
- Mode lié : utilisé pour superviser un boîtier unique lorsqu'aucun autre boîtier n'est relié. Vous pouvez utiliser le mode lié pour autoriser l'ajout de nouveaux boîtiers à mesure qu'ils sont ajoutés à l'inter-liaison. Tant qu'aucun nouveau boîtier n'est connecté, le module Onboard Administrator apparaît comme étant en mode local. Toutes les modifications de topologie qui se produisent durant une connexion sont affichées par le module Onboard Administrator. Ce mode offre une vue sans restriction des boîtiers connectés à l'inter-liaison.
- Mode fixé : utilisé pour superviser plus d'un boîtier, mais non l'ensemble des boîtiers. Seules les modifications de topologie qui affectent la topologie actuelle sont affichées par le module Onboard Administrator. Ce mode est utile lors de la surveillance d'un sous-ensemble du nombre total des boîtiers connectés à l'inter-liaison.

Si le mode actif est défini pour un boîtier unique et que un ou plusieurs boîtiers sont connectés, si vous souhaitez vous assurer que les boîtiers supplémentaires ne sont pas visibles dans la topologie des boîtiers, vous devez vous déconnecter, puis vous reconnecter sans sélectionner de boîtier lié.

Onglet Rack Topology

L'onglet Rack Topology (Topologie du rack) fournit une représentation graphique du boîtier physique que l'on appelle vue graphique. La vue graphique consiste en une vue avant et une vue arrière. Lorsque vous déplacez la souris au-dessus d'un périphérique dans la vue graphique, une fenêtre s'ouvre et affiche les informations relatives à ce périphérique. La vue graphique fournit l'état de chaque périphérique au sein du boîtier et donne la possibilité de sélectionner chacun pour obtenir des informations plus détaillées.

Sélection d'un périphérique

Pour sélectionner un périphérique, cliquez sur sa représentation graphique dans la vue graphique avant ou arrière. Lorsque vous sélectionnez un périphérique, la bordure qui l'entoure passe du gris au bleu clair pour indiquer qu'il s'agit du périphérique actuellement sélectionné. La sélection d'un périphérique en vue graphique entraîne la sélection du périphérique correspondant dans la vue de l'arborescence de navigation à gauche. Chaque fois que vous sélectionnez un périphérique à partir d'une zone du système de navigation, le reste de la navigation reflète cet événement de sélection de périphérique et se met à jour en conséquence.

Signalement des états

La vue graphique indique l'état de chaque périphérique présent dans le boîtier. Cet état est indiqué par une petite icône sur le périphérique. Aucune icône ne s'affiche pour un périphérique qui fonctionne correctement et dont l'état est normal (OK). Toutefois, tous les autres codes d'état s'affichent sous forme d'icônes sur le périphérique.

La vue graphique n'indique pas la présence ou l'absence de disques durs dans la lame de serveur ou la lame de stockage.

Sécurité du périphérique

Bien que les autorisations utilisateur aient une incidence sur les vues graphiques avant et arrière, la sécurité de la vue graphique n'est pas traitée de la même façon que dans la vue de l'arborescence à gauche. Si l'utilisateur n'est pas autorisé à accéder à un périphérique, une baie vide s'affiche, que cette baie comporte ou non un périphérique. Une icône en forme de cadenas s'affiche également dans la cellule du tableau de la baie pour indiquer que celle-ci est verrouillée pour l'utilisateur courant.

L'utilisateur ne peut pas sélectionner une baie verrouillée. Lorsque la souris passe sur une baie verrouillée, un message s'affiche pour signaler que l'utilisateur n'est pas autorisé à accéder au périphérique dans cette baie.

Informations sur le rack

Rangée	Description
Enclosure name (Nom du boîtier)	Nom configuré par l'utilisateur du boîtier dans le rack.
Enclosure Rack U Position (Position U du rack du boîtier)	Emplacement du boîtier dans le rack.
Serial Number (Numéro de série)	Numéro de série unique du boîtier.
UUID	Identifiant universel unique affecté au boîtier.
Part Number (Référence)	Référence du boîtier utilisée lors de l'obtention d'un nouveau boîtier ou d'un boîtier de remplacement.

Rangée	Description
Asset Tag (Étiquette d'inventaire)	L'étiquette d'inventaire est utilisée à des fins de contrôle des stocks.
UID State (État UID)	Affiche On ou Off selon que l'UID est actif ou non.

Pour actualiser les informations de topologie du rack, cliquez sur **Refresh Topology** (Actualiser la topologie). Lorsque l'option Refresh Topology est sélectionnée, l'écran Rack Topology bascule sur le mode lié et tous les boîtiers liés apparaissent.

Certaines informations de topologie de rack sont fournies par la solution Location Discovery Services. Pour plus d'informations sur la fonction Location Discovery Services, reportez-vous à la section « Écran Rack Overview (Présentation du rack) » (Écran Rack Overview à la page 102).

Boîtiers liés

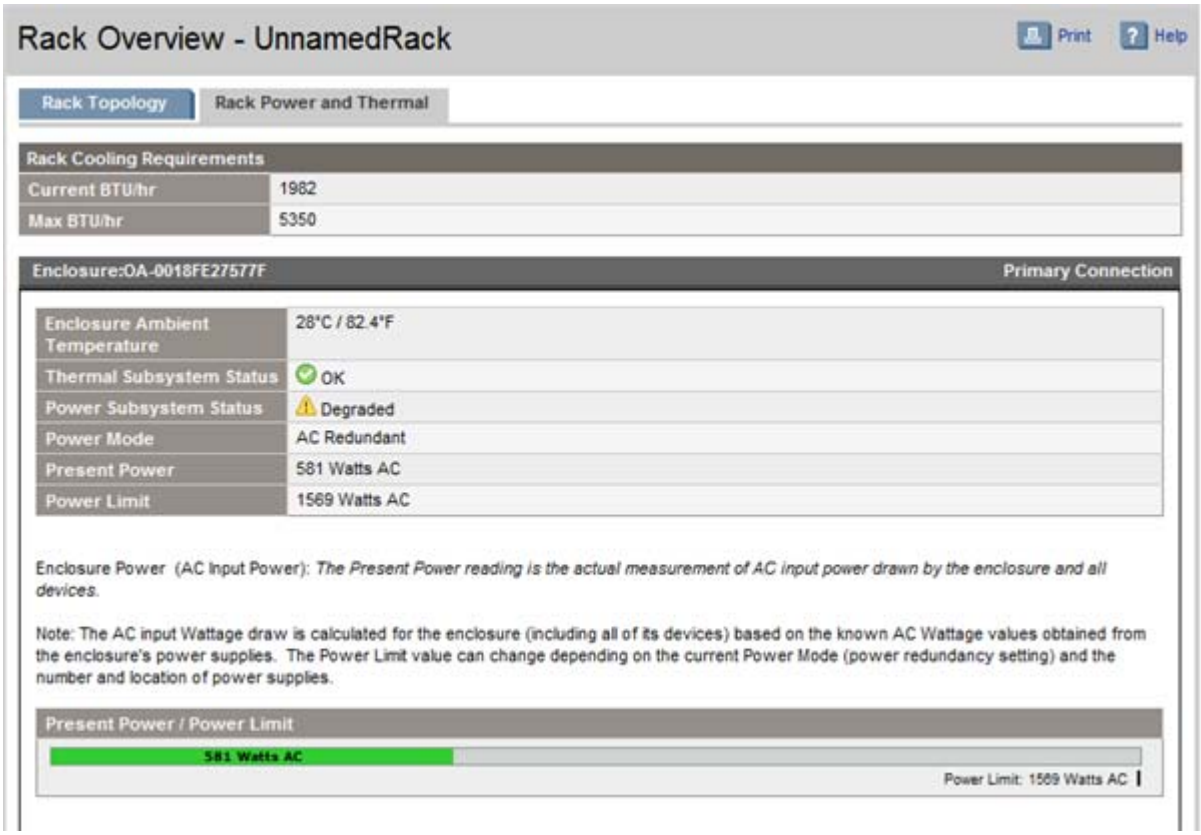
L'onglet Rack Topology (Topologie du rack) affiche tous les boîtiers liés qui ont l'un des états suivants :

- Linked - Not Signed In (Lié, non connecté). Entrez un nom d'utilisateur et un mot de passe dans les zones de texte, puis cliquez sur **Sign In** (Connexion). Une vue graphique du boîtier s'affiche.
- Linked - Not Signed In (Lié, non connecté) avec une icône de lecteur de carte. Cet état indique que le boîtier lié dispose de l'authentification à deux facteurs activée mais n'est pas authentifié. Cet état se produit sous deux conditions :
  - La configuration n'est pas prise en charge. Vous devez activer le boîtier principal pour l'authentification à deux facteurs, et les deux boîtiers (principal et lié) doivent avoir les mêmes informations d'identification pour que le boîtier lié puisse s'authentifier via l'authentification à deux facteurs.
  - Si vous cliquez sur le lien Sign Out (Déconnexion) sur un boîtier doté de l'authentification à deux facteurs qui est déjà authentifié, cet état s'affiche. Pour authentifier de nouveau ce boîtier, vous devez actualiser l'interface graphique ou authentifier à nouveau le boîtier principal.
- Linked - Signed In with a Load Enclosure Information button (Lié, connecté avec le bouton Load Enclosure Information) : cliquez sur **Load Enclosure Information** (Charger les informations du boîtier) pour afficher la vue graphique du boîtier.
- Linked - Signed In (Lié, connecté) : avec une vue graphique du boîtier affiché.

Sur le côté droit de la barre de nom du boîtier lié, cliquez sur **Sign Out** (Déconnexion) pour déconnecter ce dernier.

Onglet Rack Power and Thermal

L'onglet Rack Power and Thermal (Alimentation et température du rack) affiche des informations sur la température dans le boîtier ainsi que sur l'état d'intégrité du sous-système de température et d'alimentation. Une vue graphique de l'alimentation actuelle et de la limite de l'alimentation aide à déterminer l'état de l'alimentation.


Rack Overview - UnnamedRack
Print
Help
Rack Topology
Rack Power and Thermal
Rack Cooling Requirements
Current BTU/hr
1982
Max BTU/hr
5350
Enclosure:OA-0018FE27577F
Primary Connection
Enclosure Ambient Temperature
28°C / 82.4°F
Thermal Subsystem Status
OK
Power Subsystem Status
Degraded
Power Mode
AC Redundant
Present Power
581 Watts AC
Power Limit
1569 Watts AC
Enclosure Power (AC Input Power): The Present Power reading is the actual measurement of AC input power drawn by the enclosure and all devices.
Note: The AC input Wattage draw is calculated for the enclosure (including all of its devices) based on the known AC Wattage values obtained from the enclosure's power supplies. The Power Limit value can change depending on the current Power Mode (power redundancy setting) and the number and location of power supplies.
Present Power / Power Limit
581 Watts AC
Power Limit: 1569 Watts AC

Exigences de refroidissement du rack

Rangée	Description
Current BTU/hr (Consommation actuelle BTU/h)	Somme de la quantité de chaleur générée par les boîtiers liés, mesurée en BTU/h.
Max BTU/hr (BTU/h maxi.)	Quantité maximale de chaleur pouvant être générée par les boîtiers liés en charge, mesurée en BTU/h.

État d'alimentation et de température du boîtier

Rangée	Description
Enclosure Ambient Temperature (Température ambiante du boîtier)	Ce champ affiche la température ambiante la plus élevée reportée par les périphériques de lame installés. Si aucun périphérique de lame n'est installé, ce champ affiche la température du module Onboard Administrator en tant qu'approximation de la température ambiante.
Thermal Subsystem Status (État thermique du sous-système)	État thermique global du boîtier. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Critical Error (Erreur critique).
Power Subsystem Status (État de l'alimentation du sous-système)	État de l'alimentation globale du boîtier. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Critical Error (Erreur critique).
Power Mode (Mode d'alimentation)	Paramètre utilisateur destiné à configurer la capacité de puissance CC du boîtier et le mode de redondance d'entrée

Rangée	Description
	du boîtier. Voir la section « Gestion de l'alimentation » pour connaître les valeurs possibles.
Present Power (Puissance actuelle)	Quantité de puissance en watts consommée par tous les périphériques dans le boîtier.
Power Limit (Limite de puissance)	Puissance d'alimentation disponible pour la consommation du boîtier, mesurée en watts.
Enclosure Dynamic Power Cap (Limitation dynamique de la puissance du boîtier)	Une limite d'alimentation sur un groupe de serveurs dans le boîtier. Lorsque les serveurs fonctionnent, la demande en puissance varie en fonction de chaque serveur. Une limite de puissance est définie pour chaque serveur. Elle est suffisante pour lui permettre de faire face à sa charge de travail, mais reste conforme à la limitation dynamique de la puissance du boîtier. La surveillance continue des demandes d'alimentation et les ajustements automatiques des limites d'alimentation du serveur assurent une dégradation minimale des performances. Les informations de limitation d'alimentation dynamique du boîtier apparaissent uniquement si une limitation a été définie.

REMARQUE : Si le mode de redondance est AC Redundant ou Power Supply Redundant et que la redondance d'alimentation est perdue, vous devez ajouter des alimentations supplémentaires ou modifier le paramètre du mode de redondance dans le module Onboard Administrator pour restaurer l'état du sous-système d'alimentation. Consultez l'écran Insight Display pour connaître les mesures correctives.

Alimentation présente/Limitation d'alimentation dynamique de boîtier/Limite d'alimentation

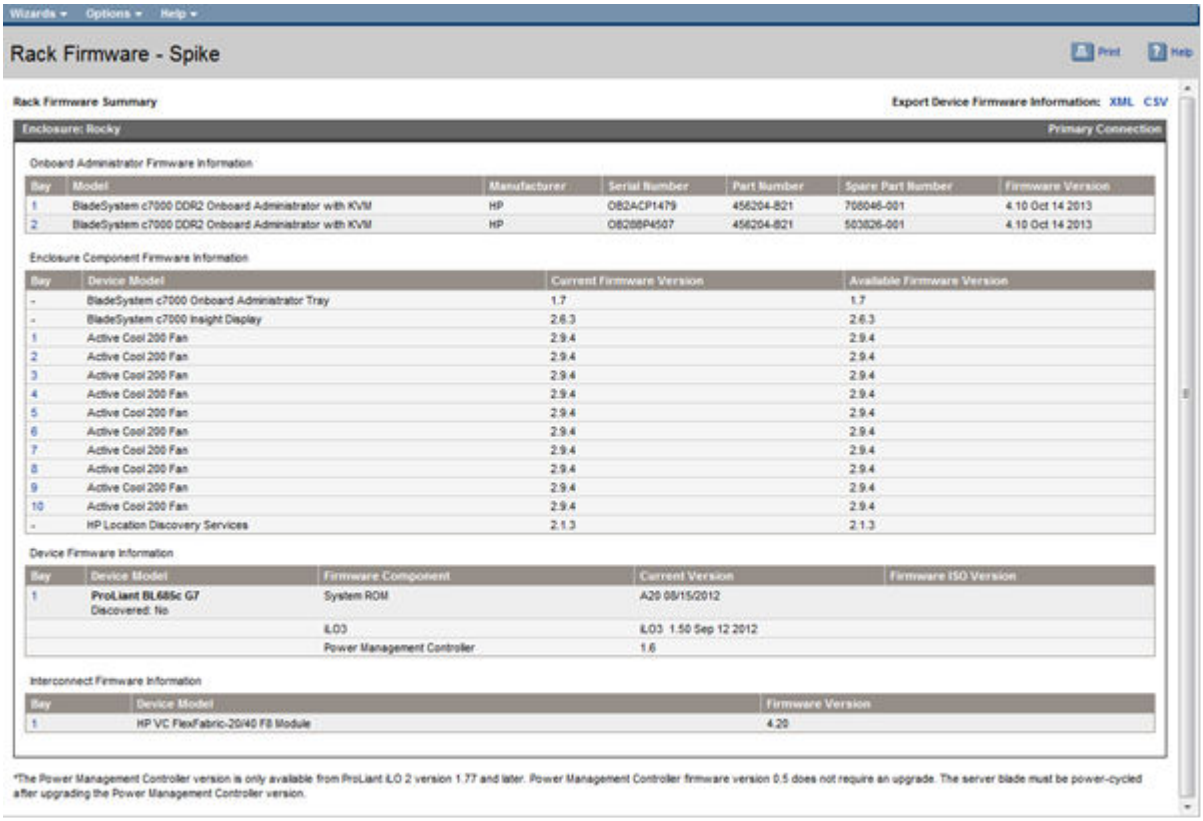
La valeur Present Power (Alimentation présente) représente la puissance en watts consommée par tous les périphériques du boîtier. La limitation d'alimentation dynamique du boîtier (Enclosure Dynamic Power Cap) ajuste automatiquement les limites d'alimentation sur les serveurs dans le boîtier pour répondre aux demandes de charge sur les serveurs tout en se conformant à la limitation d'alimentation dynamique du boîtier. La limite d'alimentation (Power Limit) est le montant maximum de puissance d'entrée disponible pour une consommation par le boîtier. La limite d'alimentation est dépendante du paramètre de redondance de puissance du boîtier et du nombre et de l'emplacement des alimentations dans le boîtier. Si une limite d'alimentation statique a été spécifiée, la limite d'alimentation affiche cette limite.

Boîtiers liés

La section Linked enclosures affiche des informations pour tous les boîtiers liés auxquels vous êtes connecté.

Écran Rack Firmware

Résumé du microprogramme du rack



REMARQUE : Pour afficher des informations complètes de version de microprogramme, une détection manuelle doit être effectuée en premier, à l'aide de l'utilitaire Enclosure Firmware Management.

Informations relatives au microprogramme du module Onboard Administrator

Colonne	Description
Bay (Baie)	Numéro de la baie physique dans laquelle le module Onboard Administrator est installé
Model (Modèle)	Numéro du modèle du module Onboard Administrator
Manufacturer (Fabricant)	Nom de la société qui a fabriqué le module Onboard Administrator
Serial Number (Numéro de série)	Numéro de série unique du module Onboard Administrator
Part Number (Référence)	Numéro de référence à utiliser pour commander un module Onboard Administrator supplémentaire ou de remplacement
Spare Part Number (Numéro de pièce de rechange)	Numéro de pièce de rechange à utiliser pour commander un module Onboard Administrator supplémentaire ou de remplacement
Firmware Version (Version du microprogramme)	Version de l'image du microprogramme dans le module Onboard Administrator

Informations relatives aux microprogrammes des composants du boîtier

Colonne	Description
Bay (Baie)	Numéro de la baie physique dans laquelle le composant est installé
Device Model (Modèle du périphérique)	Numéro de modèle du périphérique
Current Firmware Version (Version actuelle du microprogramme)	Version du microprogramme installé sur le composant
Available Firmware Version (Version disponible du microprogramme)	Dernière version du microprogramme disponible pour installation sur le composant

Informations relatives aux microprogrammes des périphériques

Colonne	Description
Bay (Baie)	Numéro de la baie physique dans laquelle le périphérique est situé dans le boîtier
Device Model (Modèle du périphérique)	Modèle du périphérique. La date de la détection plus récente du microprogramme s'affiche, ou si aucune détection n'a été effectuée sur ce périphérique, `No` (Non) apparaît.
Firmware Component (Composant du microprogramme)	Le nom de chaque composant est répertorié sur des lignes séparées. Les composants pris en charge par le DVD Firmware sont répertoriés, notamment : • ROM système • iLO • Contrôleur de supervision d'alimentation • Cartes réseau • HBA • Smart Array et disques durs reliés Pour les composants ayant plusieurs versions de microprogramme interne tels que les cartes réseau, chacune de ces versions est indiquée séparément.
Current Version (Version actuelle)	Version actuelle du microprogramme de ce composant.
Firmware DVD Version (Version DVD du microprogramme)	Version du DVD Firmware de ce composant.

Informations relatives aux microprogrammes d'interconnexion

Colonne	Description
Bay (Baie)	Numéro de la baie physique dans laquelle l'interconnexion est située dans le boîtier
Device Model (Modèle du périphérique)	Modèle de l'interconnexion
Firmware Version (Version du microprogramme)	Version de microprogramme du module d'interconnexion. `Not Available` (non disponible) apparaît lorsque le module d'interconnexion ne fournit pas les informations relatives à la version de microprogramme.

Exporter les Informations relatives aux microprogrammes

Pour exporter les informations relatives à la version de microprogramme qui apparaissent sur cet écran au format CSV ou XML, cliquez sur **XML** ou **CSV.**

REMARQUE : L'option CSV est disponible uniquement avec Internet Explorer.

REMARQUE : Si le microprogramme de la lame ne correspond pas au microprogramme de l'image ISO du DVD une fois un serveur détecté ou mis à jour, une icône d'information s'affiche.

REMARQUE : Une lettre incluse après la version du microprogramme indique une révision de note de version du composant intelligent. Cette révision n'est pas une mise à jour fonctionnelle du microprogramme.

8 Configuration des boîtiers HP BladeSystem et des périphériques de boîtier

Affichage des écrans d'état

Il est possible de sélectionner chaque boîtier dans l'arborescence de gauche. Si vous cliquez sur le nom du boîtier, sa page principale d'état s'affiche.

Sur cette page, quatre onglets sont disponibles en haut de la page principale : Status (État), Information (Informations), Virtual Buttons (Boutons virtuels) et Component Firmware (Microprogramme du composant).

L'onglet Status (État) affiche l'une des valeurs suivantes pour l'état global du boîtier :

- Critical/Failed (Critique/Échec)
- Major (Majeur)
- Minor/Degraded (Mineur/Détérioré)
- Normal/OK
- Unknown (Inconnu)
- Information

L'état du module HP BladeSystem Onboard Administrator actif et l'état du module HP BladeSystem Onboard Administrator en mode Standby sont similaires à l'état global du boîtier. Ils affichent l'état du module Onboard Administrator. Si un module Onboard Administrator en mode Standby est absent du système, son état a la valeur Absent.

Le mode Enclosure Power (Alimentation du boîtier) affiche le mode d'alimentation courant du boîtier. Les valeurs suivantes sont possibles :

- AC Redundant (Redondance secteur)
- Power Supply Redundant (Redondance d'alimentation)
- Not Redundant (Non redondant)

L'écran Enclosure Status Overview (Présentation de l'état du boîtier) se compose de quatre sections :

- Device Bay Overview (Présentation de la baie de périphérique)
- Interconnect Bay Overview (Présentation de la baie d'interconnexion)
- Power Subsystem (Sous-système d'alimentation)
- Thermal Subsystem (Sous-système thermique)

Pour chacune de ces sections, les valeurs suivantes sont possibles :

- Critical/Failed (Critique/Échec)
- Major (Majeur)

- Minor/Degraded (Mineur/Détérioré)
- Normal/OK
- Unknown (Inconnu)
- Information

Paramètres du boîtier

Sélection de boîtiers

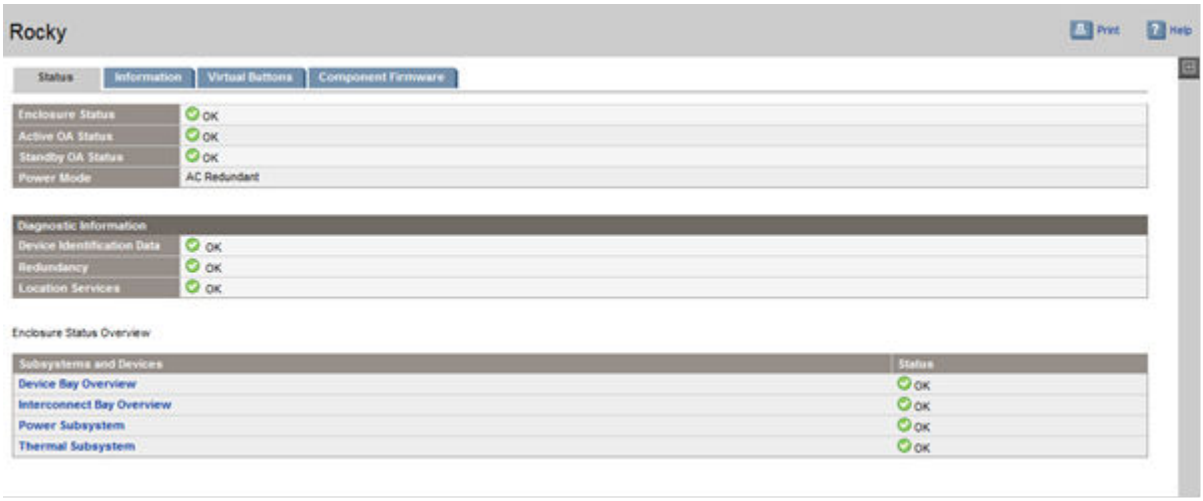
Les ports principaux d'inter-liaison sont affichés dans le tableau de topologie du rack. Le boîtier principal est sélectionné par défaut, et ne peut pas être désélectionné.

Lorsque les boîtiers liés sont affichés, le mode de topologie utilisé par l'application au cours de votre session est déterminé par les sélections de case à cocher effectuées avant la connexion, comme décrit ci-dessous :

- Mode local : mode de topologie par défaut. Activé si aucun des boîtiers liés n'est sélectionné. Toutes les modifications de topologie qui se produisent lorsque connecté sont ignorées par l'application.
- Mode fixé : ce mode de topologie est activé lorsque certains des boîtiers liés sont sélectionnés, mais pas l'ensemble. Seules les modifications de topologie qui affectent les boîtiers sélectionnés lorsque connecté sont affichées par l'application.
- Mode lié : ce mode de topologie est activé si tous les boîtiers affichés sont sélectionnés. Toutes les modifications de topologie qui se produisent lorsque connecté sont affichées par l'application.

Écran Enclosure Information

Pour afficher des informations sur le boîtier, sélectionnez **Enclosure Information** à partir de la vue d'arborescence. L'écran d'informations sur le boîtier inclut quatre onglets : **Status**, **Information**, **Virtual Buttons** et **Component Firmware**.



Onglet Enclosure Status

Informations d'état

Rangée	Description
Enclosure Status (État du boîtier)	État global du boîtier. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré), N/A ou Critical Error (Erreur critique).*
Active OA Status (État du OA actif)	État global du module Onboard Administrator actif. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Failed (Échec).
Standby OA Status (État du OA en mode Standby)	État global du module Onboard Administrator en mode Standby. Les valeurs possibles sont Absent, Unknown (Inconnu), OK, Degraded (Détérioré) ou Failed (Échec).
Power Mode (Mode d'alimentation)	Paramètre utilisateur destiné à configurer la capacité de puissance CC du boîtier et le mode de redondance d'entrée du boîtier. Voir la section « Gestion de l'alimentation » pour connaître les valeurs possibles.

* L'état du boîtier apparaît comme N/A si le paramètre Enable Extended Data on GUI Login Page (Activer les données étendues sur la page de connexion à l'interface graphique) est désactivé. Ce paramètre est accessible via Enclosure Settings>Network Access>Anonymous Data (Paramètres du boîtier>Accès au réseau>Données anonymes).

Informations relatives aux diagnostics de boîtier

Les informations de diagnostics sont recueillies de deux façons : Par interrogation du microcontrôleur de périphérique (résultat d'un état détérioré si une panne s'est produite) ou envoyées par le microcontrôleur du périphérique, sans interrogation, pour signaler une panne.

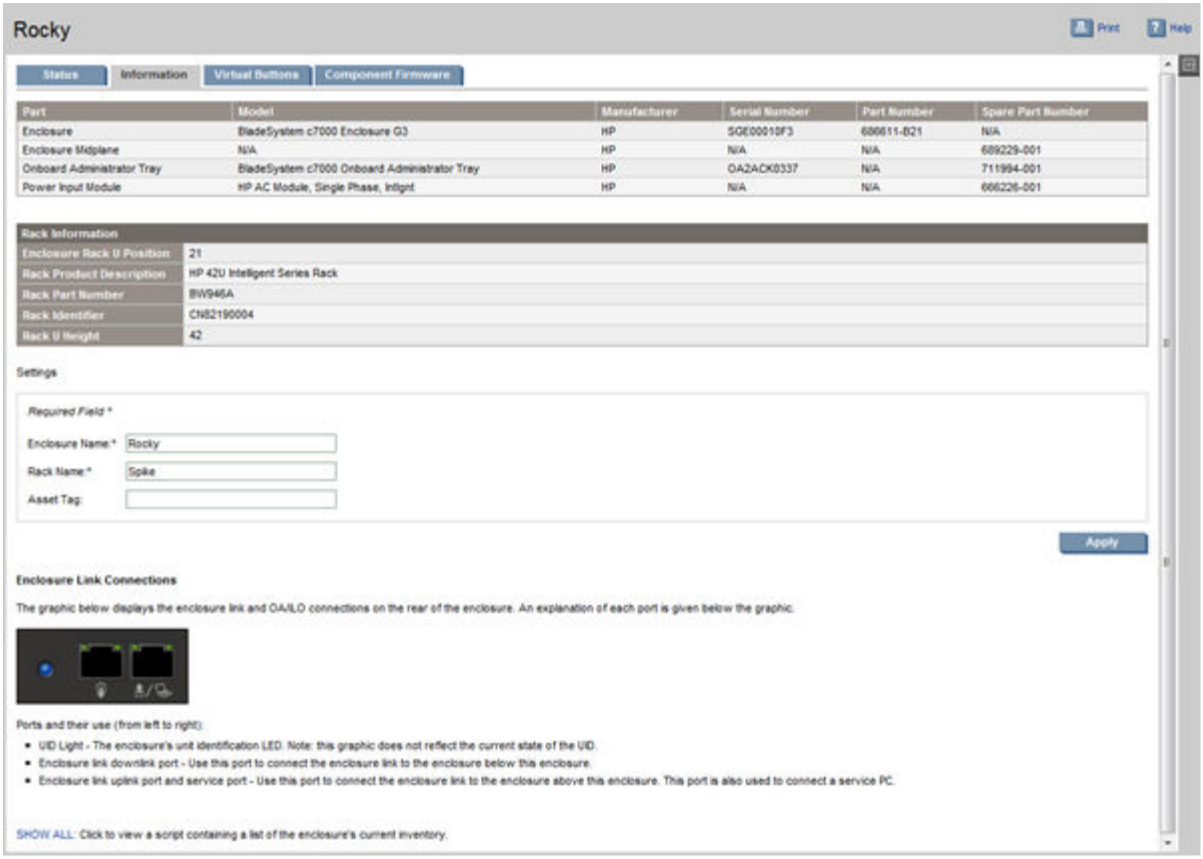
Rangée	Description
Device Identification Data (Données d'identification du périphérique)	Contient des informations telles que le nom du modèle, la référence, le numéro de série, ainsi que d'autres informations utilisées pour identifier le périphérique. Ces données sont également appelées données FRU. Une erreur de données d'identification du périphérique s'affiche si les données sont absentes ou illisibles par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Redundancy (Redondance)	Les valeurs possibles sont OK et Error. Une erreur indique que les modules Onboard Administrator redondants présentent des problèmes de synchronisation. Consultez le journal système pour plus d'informations sur les erreurs. Des raisons possibles de l'erreur incluent une discordance de microprogramme ou un défaut matériel ou logiciel.
Location Services (Services d'emplacement)	Les valeurs possibles sont OK ou Other (Autre). Other indique qu'une erreur de services d'emplacement s'est produite. Des données peuvent être corrompues.

Présentation des états du boîtier

Sous-systèmes et périphériques	Description
Device Bay Overview (Présentation de la baie de périphérique)	État global de toutes les baies de périphérique. L'état est un état global de tous les périphériques dans le boîtier. Si plusieurs périphériques ont un état autre que OK, ils sont affichés dans une liste dans ce tableau.
Interconnect Bay Overview (Présentation de la baie d'interconnexion)	État global des baies d'interconnexion. L'état est un état global de toutes les interconnexions dans le boîtier. Si

Sous-systèmes et périphériques	Description
	plusieurs interconnexions ont un état autre que OK, elles sont affichées dans une liste dans ce tableau.
Power Subsystem (Sous-système d'alimentation)	État global du sous-système d'alimentation du boîtier. L'état est un état global de toutes les alimentations dans le boîtier. Si plusieurs alimentations ont un état autre que OK, elles sont affichées dans une liste dans ce tableau.
Thermal Subsystem (Sous-système thermique)	État global du sous-système thermique du boîtier. L'état est un état global de tous les ventilateurs dans le boîtier. Si plusieurs ventilateurs ont un état autre que OK, ils sont affichés dans une liste dans ce tableau.

Informations relatives au boîtier



Informations matérielles

Colonne	Description
Part (Pièce)	Nom de la pièce
Model (Modèle)	Numéro de modèle de la pièce
Manufacturer (Fabricant)	Nom de la société qui a fabriqué la pièce
Serial Number (Numéro de série)	Numéro de série unique de la pièce
Part Number (Référence)	Référence à utiliser pour commander une pièce supplémentaire. Le module d'entrée d'alimentation n'a pas

Colonne	Description
	de numéro de pièce et affiche toujours N/A dans la colonne Part Number (Référence).
Spare Part Number (Numéro de la pièce de rechange)	Référence à utiliser pour commander une pièce de remplacement.

Informations sur le rack

Rangée	Description
Enclosure Rack U Position (Position U du rack du boîtier)	Emplacement du boîtier dans le rack.
Rack Product Description (Description du produit du rack)	Nom descriptif commun du rack.
Rack Part Number (Référence du rack)	Référence à utiliser pour commander un rack de remplacement.
Rack Identifier (Identificateur du rack)	Chaîne unique qui identifie le rack.
Rack U Height (Hauteur U du rack)	Hauteur U du rack.

Cela inclut des informations recueillies par la fonction Location Discovery Services. Pour plus d'informations sur l'utilisation de la fonction Location Discovery Services, reportez-vous à la section « Écran Rack Overview (Présentation du rack) » (Écran Rack Overview à la page 102).

Modifications de paramètres

Les paramètres du boîtier peuvent être modifiés à partir de cet écran. Pour enregistrer les paramètres après avoir apporté des modifications, cliquez sur **Apply** (Appliquer).

Champ	Valeur possible	Description
Enclosure name (Nom du boîtier)	De 1 à 32 caractères, notamment tous les caractères alphanumériques, le tiret (-) et le trait de soulignement (_).	Nom du boîtier sélectionné.
Rack Name (Nom du rack)	De 1 à 32 caractères, notamment tous les caractères alphanumériques, le tiret (-) et le trait de soulignement (_).	Nom du rack sur lequel le boîtier est installé.
Asset Tag (Étiquette d'inventaire)	De 0 à 32 caractères, notamment tous les caractères alphanumériques, le tiret (-) et le trait de soulignement (_).	L'étiquette d'inventaire est utilisée à des fins de contrôle des stocks. L'étiquette par défaut est vierge.

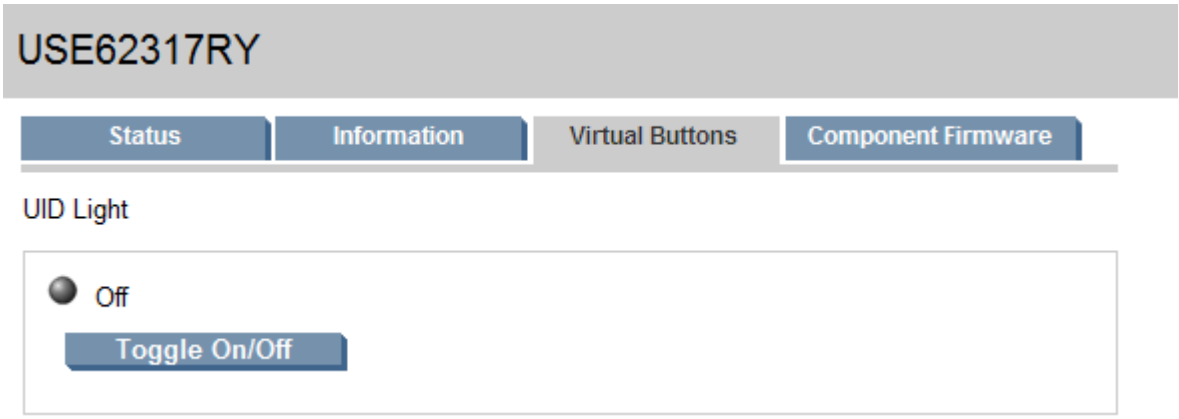
Connexions de liaison du boîtier

Cette section fournit une vue graphique des connexions de liaison du boîtier, situées à l'arrière du boîtier, et des informations détaillées sur chaque port de liaison du boîtier.

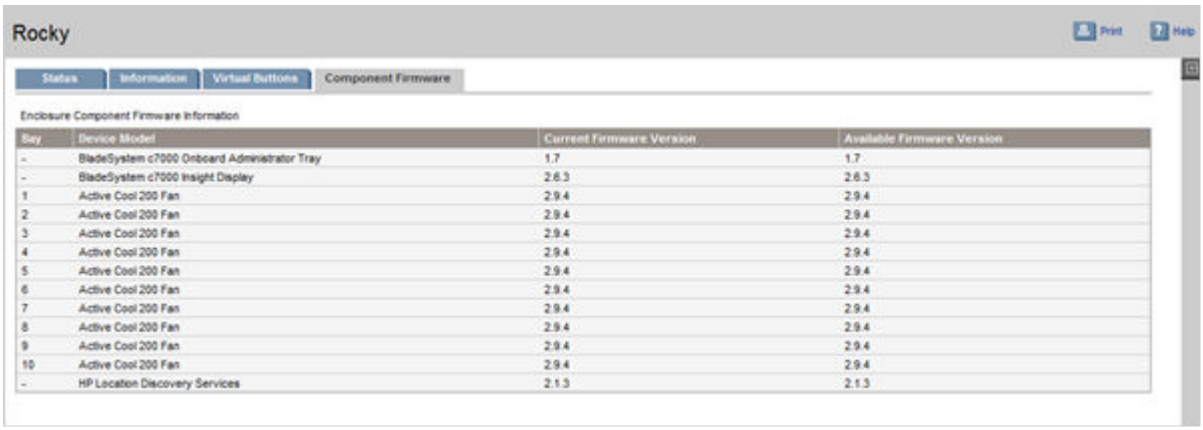
Pour afficher un script contenant une liste du répertoire actuel du boîtier, cliquez sur **SHOW ALL** (Afficher tout).

Boutons virtuels

Pour modifier l'état du voyant UID du boîtier, situé en regard de la liaison du boîtier et des connexions Onboard Administrator/iLO, cliquez sur **Toggle On/Off** (Activer/Désactiver).



Microprogramme du composant


Rocky
Print
Help
Status
Information
Virtual Buttons
Component Firmware
Enclosure Component Firmware Information
Bay
Device Model
Current Firmware Version
Available Firmware Version
- BladeSystem c7000 Onboard Administrator Tray 1.7 1.7
- BladeSystem c7000 Insight Display 2.6.3 2.6.3
1 Active Cool 200 Fan 2.9.4 2.9.4
2 Active Cool 200 Fan 2.9.4 2.9.4
3 Active Cool 200 Fan 2.9.4 2.9.4
4 Active Cool 200 Fan 2.9.4 2.9.4
5 Active Cool 200 Fan 2.9.4 2.9.4
6 Active Cool 200 Fan 2.9.4 2.9.4
7 Active Cool 200 Fan 2.9.4 2.9.4
8 Active Cool 200 Fan 2.9.4 2.9.4
9 Active Cool 200 Fan 2.9.4 2.9.4
10 Active Cool 200 Fan 2.9.4 2.9.4
- HP Location Discovery Services 2.1.3 2.1.3

Colonne	Description
Bay (Baie)	Baie du périphérique dans le boîtier.
Device Model (Modèle du périphérique)	Numéro de modèle du périphérique
Current Firmware Version (Version actuelle du microprogramme)	Version du microprogramme installé du périphérique
Available Firmware Version (Version disponible du microprogramme)	Dernière version du microprogramme actuellement disponible pour le périphérique

L'onglet Enclosure Component Firmware (Microprogramme de composant du boîtier) indique également la version du microprogramme du PIC d'emplacement (périphérique d'emplacement BladeSystem), telle que fournie par Location Discovery Services. Pour plus d'informations sur l'utilisation de la fonction Location Discovery Services, reportez-vous à la section « Écran Rack Overview (Présentation du rack) » (Écran Rack Overview à la page 102).

AlertMail

AlertMail permet aux utilisateurs de recevoir les événements système par courrier électronique plutôt que par interruption SNMP. AlertMail est entièrement indépendant de SNMP mais les deux systèmes peuvent être activés simultanément. AlertMail utilise les commandes SMTP standard pour communiquer avec un serveur de messagerie compatible SMTP. L'adresse de réponse « reply to »

de chaque courrier envoyé par AlertMail sera <Nom_boîtier>@<Domaine_expéditeur_alerte>. Pour activer la fonction AlertMail, cochez la case **Enable AlertMail**.

Pour tester la fonction AlertMail, assurez-vous que les paramètres d'adresse électronique, de domaine de l'expéditeur d'alerte et du serveur SMTP sont corrects. Sélectionnez **Send Test AlertMail** (Envoyer test AlertMail). Pour confirmer le succès du test, vérifiez le compte de messagerie du destinataire.

REMARQUE : Le champ Alert Sender Domain (Domaine de l'expéditeur de l'alerte) n'est peut-être pas nécessaire. Ce champ dépend de l'installation de serveur de messagerie.

Champ	Valeur possible	Description
E-Mail address (Adresse électronique)	<compte>@<domaine>	Adresse électronique valide pour l'administrateur ou toute autre personne désignée pour recevoir le message d'alerte
SMTP Server (Serveur SMTP)	• Adresse IPv4 : ###.###.###.### où ### est compris entre 0 et 255. • Adresse Ipv6 : ####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. • Nom DNS : peut comprendre entre 1 et 64 caractères notamment tous les caractères alphanumériques et le tiret (-)	Une adresse IPv4, une adresse IPv6 ou le nom DNS du serveur SMTP
Alert Sender Name (Nom de l'expéditeur de l'alerte)	Une chaîne de caractères comprenant tous les caractères alphanumériques, le tiret (-), le trait de soulignement (_) et l'espace. Le champ est facultatif avec une limite de 40 caractères.	Nom du module Onboard Administrator
Alert Sender Domain (Domaine de l'expéditeur de l'alerte)	Chaîne de caractères, y compris tous les caractères alphanumériques, le tiret (-) et le point (.)	Domaine dans lequel réside le module Onboard Administrator. Mutuellement exclusif avec Sender Email (Courrier électronique de l'expéditeur)
Alert Sender E-mail (E-mail de l'expéditeur de l'alerte)	<compte>@<domaine>	Adresse électronique valide de l'expéditeur pour l'administrateur ou toute autre personne désignée pour recevoir le message d'alerte.

1. Cochez la case **Enable AlertMail** pour activer la fonctionnalité AlertMail.
2. Entrez les valeurs de l'adresse de messagerie, du domaine de l'expéditeur de l'alerte et du serveur SMTP.
3. Cliquez sur **Apply** (Appliquer) pour enregistrer les paramètres.

Lorsqu'il est activé, AlertMail envoie une alerte par messagerie électronique pour les événements suivants :

- Changement d'état du boîtier
- Modification des informations relatives au boîtier
- Changement d'état d'un ventilateur
- Ventilateur inséré
- Ventilateur supprimé
- État de l'alimentation
- Bloc d'alimentation inséré
- Bloc d'alimentation supprimé
- Surcharge du bloc d'alimentation
- Lame insérée
- Lame supprimée
- État de la lame
- Condition thermique de la lame
- Erreur de lame
- Modification des informations relatives à la lame
- Modification de l'état du plateau
- Réinitialisation du plateau
- Connexion du commutateur
- Déconnexion du commutateur

Tous les messages ont l'en-tête suivant :

```
From: Enclosure ENCLOSURE-NAME <enclosure-name@serverdomain>

Date: Date in standard format

Subject: HP AlertMail-SEQ: <SEVERITY> SUBJECT

To: RECEIVER MAILBOX
```

Où SEVERITY (degré de sévérité) peut prendre l'une des valeurs suivantes (du plus élevé au plus faible) :

- # FATAL
- # CRITICAL (CRITIQUE)
- # WARNING MAJOR (AVERTISSEMENT MAJEUR)
- # WARNING MINOR (AVERTISSEMENT MINEUR)

- # WARNING (AVERTISSEMENT)
- # NORMAL

Chaque ligne d'objet contient un numéro de séquence unique pour identifier aisément l'ordre des événements au cas où le serveur de messagerie distribuerait les messages dans un ordre incorrect. Les numéros de séquence sont compris entre 0 et 999 et démarrent à nouveau à 0.

Le corps du message est utilisé pour fournir plus d'informations détaillées sur l'événement émis. Il contient également des informations sur les actions que l'utilisateur doit entreprendre pour corriger un problème ainsi que sur l'état du boîtier courant.

REMARQUE : L'état du boîtier affiché correspond à l'état au moment où l'événement a été traité ce qui signifie que l'état peut être normal dans un message annonçant une panne de ventilateur si l'utilisateur a déjà remplacé le ventilateur au moment où l'événement a été envoyé par AlertMail.

Exemple de message

```
Subject: HP AlertMail-010: (CRITICAL) Power Supply #1: Failed

Date: Wed, 23 Apr 2006 15:02:22 +0200

From: Enclosure EM-00508BEBA571 <EM-00508BEBA571@hp.com>

To: user@domain

X-OS: HP BladeSystem Enclosure Manager

X-Priority: 1

Content-Type: text/plain; charset=us-ascii

EVENT (26 May 07:09): Power Supply #1 Status has changed to: Failed.

Enclosure, EM-00508BEBA571, has detected that a power supply in bay 1 has
changed from status OK to Failed.

The power supply should be replaced with the appropriate spare part. You
can ensure that the center wall assembly is operating correctly by
swapping the two power supplies. Make sure that there are no bent pins on
the power supply connectors before reinserting and that each power supply
is fully seated.

An amber LED on the power supply indicates either an over-voltage, over-
temperature, or loss of AC power has occurred. A blinking LED on the
power supply indicates a current limit condition.

Enclosure Status: Degraded

Enclosure Management URL: https://16.181.75.213/

- PLEASE DO NOT REPLY TO THIS EMAIL -
```

Onglets de baies de périphériques de séquence d'alimentation de périphériques

La fonctionnalité du délai de l'alimentation du boîtier contrôle l'ordre dans lequel les composants sont sous tension si l'ensemble du boîtier a été mis hors puis sous tension. Cette fonctionnalité est activée uniquement pendant la procédure de démarrage du module HP BladeSystem Onboard Administrator

actif si le module Onboard Administrator détecte que l'ensemble du boîtier a été mis hors puis sous tension et que le délai de l'alimentation a été activé sur au moins un composant dans le boîtier.

Le module HP BladeSystem Onboard Administrator actif affiche un message dans le journal système lorsque le délai d'alimentation a été initialisé, ainsi qu'un autre message dans le journal système à l'issue du délai d'alimentation après que le plus long délai d'alimentation a expiré. Le paramètre par défaut d'usine pour le module HP BladeSystem Onboard Administrator désactive le délai d'alimentation pour tous les composants.

Cas d'utilisation typiques qui impliquent des dépendances de baie à baie pouvant être résolues en activant la fonction du délai de l'alimentation du boîtier :

- **Démarrage à partir du réseau** : Les interconnexions de réseau doivent d'abord terminer l'opération POST (power on self test) sur les serveurs configurés pour un démarrage à partir du réseau (par exemple, PXE ou iSCSI).
- **Démarrage depuis le réseau SAN** : interconnexions de réseau SAN doit d'abord terminer l'opération POST (power on self test) avant les serveurs configurés pour démarrer depuis le réseau SAN.
- Dépendances de service critiques contrôlées par un serveur telles que DHCP ou un contrat de licence
- Les serveurs de stockage doivent être opérationnels avant les serveurs qui nécessitent ces ressources

Le paramètre de délai doit être déterminé empiriquement puisque certaines dépendances sont à l'extérieur du boîtier (le démarrage depuis le réseau SAN peut nécessiter un délai supplémentaire pour permettre la mise sous tension du système de stockage du réseau SAN du centre de données). Chaque module d'interconnexion a un temps de mise sous tension différent avant d'être opérationnel.

L'horloge utilisée pour le délai d'alimentation est démarrée au moment où le module Onboard Administrator crée le premier message de journal système pendant l'initialisation du module Onboard Administrator indiquée par le message `Kernel: Network link up`. Lorsque le module HP BladeSystem Onboard Administrator indique `PowerDelay has been initiated for the selected devices` (Le délai d'alimentation a été initialisé pour les périphériques sélectionnés) dans le journal système, les délais configurés pour chaque baie sont utilisés pour déterminer quand ce composant est activé. Une fois le délai sélectionné expiré, ce composant est activé.

Les paramètres valides pour chaque baie sont : Disabled (Désactivé), Enabled (Activé) et No Poweron (Aucune alimentation).

Disabled : désactive le délai d'alimentation pour cette baie. Le module HP BladeSystem Onboard Administrator alimente cette baie en fonction de ses paramètres d'alimentation : pour un périphérique configuré sur mise sous tension automatique, le périphérique alimente suivant un cycle d'alimentation de boîtier après avoir terminé toutes les vérifications de configuration du module Onboard Administrator.

Enabled : active le délai d'alimentation pour cette baie. Le module HP BladeSystem Onboard Administrator active cette baie selon le nombre de secondes écoulé après la détection d'un événement de mise hors puis sous tension du boîtier.

No Poweron (Aucune alimentation) : Empêche la mise sous tension du composant pour les baies avec cette configuration jusqu'à la création par le module HP BladeSystem Onboard Administrator d'un message `PowerDelay has completed for the selected devices` (Le délai d'alimentation a expiré pour les périphériques sélectionnés). À ce moment, si le périphérique est configuré pour la mise sous tension automatique, il accorde alors l'alimentation après une mise hors puis sous tension du boîtier et après que tous les contrôles de configuration du module Onboard Administrator ont été terminés.

Si le périphérique est configuré pour désactiver la mise sous tension automatique, il reste alors hors tension après une mise hors puis sous tension du boîtier quel que soit le paramètre de délai d'alimentation pour cette baie.

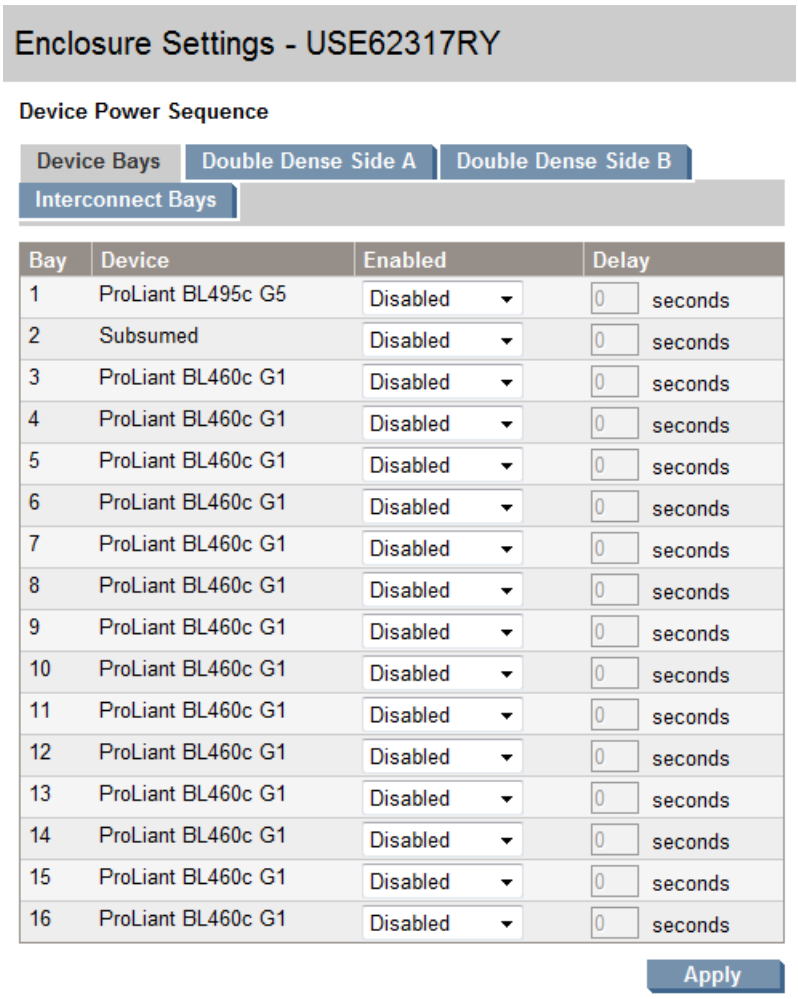
Onglet standard de baies de périphériques et onglets Double densité

L'onglet Device Bays Standard (Standard des baies de périphérique) indique les paramètres actuels pour toutes les baies principales selon le type de boîtier. Pour modifier un paramètre sur une baie de périphérique donnée, utilisez le menu sous la colonne Enabled (Activé) et sélectionnez Enabled (Activé), Disabled (Désactivé) ou No Poweron (Aucune alimentation). Si Enabled (Activé) est sélectionné, un délai d'alimentation en secondes doit être entré dans la colonne Delay (Délai) pour cette baie. La valeur minimale est 1 seconde et la valeur maximale 3600.

Si des serveurs double densité sont installés dans un boîtier, les paramètres du délai d'alimentation pour le côté A et le côté B sont contrôlés dans les onglets Double Dense Side A et Double Dense Side B (Côté A double densité et Côté B double densité).

Onglet Interconnect Bays

Par défaut, les baies d'interconnexion correspondent au paramètre de mise sous tension automatique. L'activation et la définition d'un délai d'alimentation pour une baie d'interconnexion diffère la mise sous tension de cette baie après une mise hors puis sous tension du boîtier.


Enclosure Settings - USE62317RY
Device Power Sequence
Device Bays
Double Dense Side A
Double Dense Side B
Interconnect Bays
Bay
Device
Enabled
Delay
1 ProLiant BL495c G5 Disabled 0 seconds
2 Subsumed Disabled 0 seconds
3 ProLiant BL460c G1 Disabled 0 seconds
4 ProLiant BL460c G1 Disabled 0 seconds
5 ProLiant BL460c G1 Disabled 0 seconds
6 ProLiant BL460c G1 Disabled 0 seconds
7 ProLiant BL460c G1 Disabled 0 seconds
8 ProLiant BL460c G1 Disabled 0 seconds
9 ProLiant BL460c G1 Disabled 0 seconds
10 ProLiant BL460c G1 Disabled 0 seconds
11 ProLiant BL460c G1 Disabled 0 seconds
12 ProLiant BL460c G1 Disabled 0 seconds
13 ProLiant BL460c G1 Disabled 0 seconds
14 ProLiant BL460c G1 Disabled 0 seconds
15 ProLiant BL460c G1 Disabled 0 seconds
16 ProLiant BL460c G1 Disabled 0 seconds
Apply

Colonne	Description
Bay (Baie)	Numéro de baie du périphérique.
Device (Périphérique)	Type de périphérique dans la baie, ou Absent si aucun périphérique n'est installé dans la baie.
Enabled (Activé)	Active le séquencement d'alimentation, désactive le séquencement d'alimentation, ou n'autorise pas l'alimentation du périphérique si l'option No Poweron est sélectionnée.
Delay (Délai)	Durée du délai, en secondes, avant la mise sous tension du périphérique.

Onglet de baies d'interconnexion de séquence d'alimentation de périphériques

Colonne	Description
Bay (Baie)	Numéro de baie du périphérique.
Device (Périphérique)	Type de périphérique dans la baie, ou Absent si aucun périphérique n'est installé dans la baie.
Enabled (Activé)	Active le séquencement d'alimentation, désactive le séquencement d'alimentation, ou n'autorise pas l'alimentation du périphérique si l'option No Poweron est sélectionnée.
Delay (Délai)	Durée du délai, en secondes, avant la mise sous tension du périphérique. Les valeurs de délai possibles vont de 1 à 3600.

Cliquez sur **Apply** (Appliquer) pour enregistrer les paramètres.

Date et heure

Paramètres de date et heure statiques

La date et l'heure sont statiques et ne sont pas mises à jour en temps réel. La date et l'heure ne peuvent être définies que si NTP est désactivé.

Champ	Valeur possible	Description
Date	aaaa-mm-jj • mm est un entier compris entre 1 et 12 • jj est un entier compris entre 1 et 31	Date attribuée au boîtier
Time (Heure)	hh:mm:ss (format 24 heures, ss en option) • hh est un entier compris entre 0 et 23	Heure attribuée au boîtier

Champ	Valeur possible	Description
	• mm est un entier compris entre 0 et 59	
Time Zone (Fuseau horaire)	Paramètres des fuseaux horaires • Paramètres de fuseaux horaires de la zone Afrique (Paramètres de fuseaux horaires de la zone Afrique à la page 433) • Paramètres de fuseaux horaires de la zone Amérique (Paramètres de fuseaux horaires de la zone Amérique à la page 434) • Paramètres de fuseaux horaires de la zone Asie (Paramètres de fuseaux horaires de la zone Asie à la page 436) • Paramètres de fuseaux horaires universels (Paramètres de fuseaux horaires universels à la page 433) • Paramètres des fuseaux horaires des zones océaniques (Paramètres de fuseaux horaires de la zone Océanie à la page 437) • Paramètres de fuseaux horaires de la zone Europe (Paramètres de fuseaux horaires de la zone Europe à la page 438) • Paramètres de fuseaux horaires de la zone polaire (Paramètres de fuseaux horaires de la zone polaire à la page 438)	Fuseau horaire attribué au boîtier

Paramètres NTP

Pour activer cette fonction, sélectionnez **Set time using an NTP server** (Définir l'heure à l'aide d'un serveur NTP).

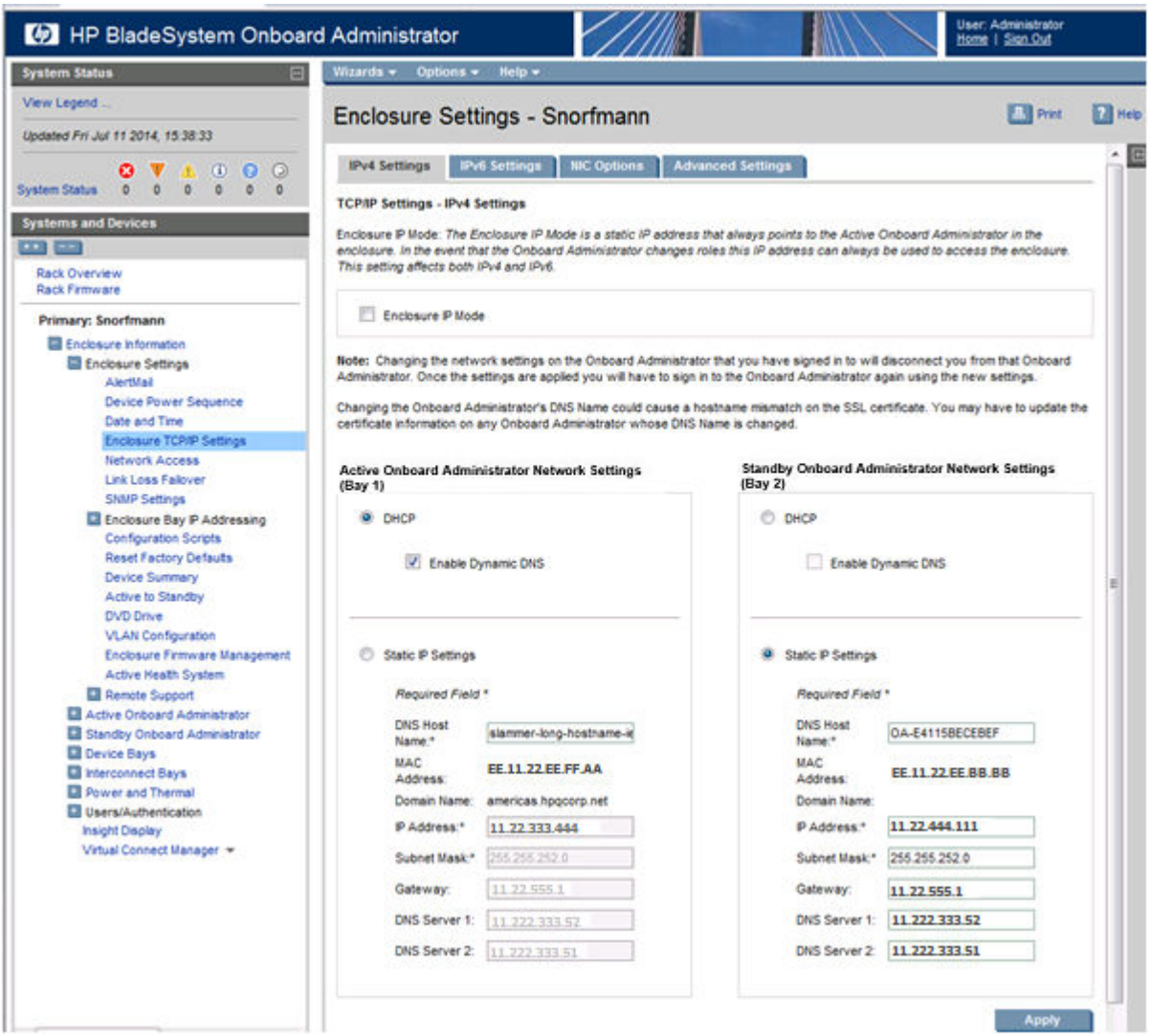
Champ	Valeur possible	Description
Primary NTP Server (Serveur NTP principal)	• Adresse IPv4 : ###.###.###.### où ### est compris entre 0 et 255. • Adresse Ipv6 : ####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. • Nom DNS : peut comprendre entre 1 et 64 caractères notamment tous les caractères alphanumériques et le tiret (-).	Adresse IP ou nom DNS du serveur NTP principal qui fournit les informations de date et heure
Secondary NTP Server (Serveur NTP secondaire)	• Adresse IPv4 : ###.###.###.### où ### est compris entre 0 et 255.	Adresse IP ou nom DNS du serveur NTP secondaire qui fournit les informations de date et heure

Champ	Valeur possible	Description
	• Adresse Ipv6 : ####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. • Nom DNS : peut comprendre entre 1 et 64 caractères notamment tous les caractères alphanumériques et le tiret (-).	
Poll Interval (Intervalle d'interrogation)	Entier compris entre 60 et 86400	Intervalle de scrutation en secondes du serveur NTP
Time Zone (Fuseau horaire)	Paramètres des fuseaux horaires • Paramètres de fuseaux horaires de la zone Afrique (Paramètres de fuseaux horaires de la zone Afrique à la page 433) • Paramètres de fuseaux horaires de la zone Amérique (Paramètres de fuseaux horaires de la zone Amérique à la page 434) • Paramètres de fuseaux horaires de la zone Asie (Paramètres de fuseaux horaires de la zone Asie à la page 436) • Paramètres de fuseaux horaires universels (Paramètres de fuseaux horaires universels à la page 433) • Paramètres des fuseaux horaires des zones océaniques (Paramètres de fuseaux horaires de la zone Océanie à la page 437) • Paramètres de fuseaux horaires de la zone Europe (Paramètres de fuseaux horaires de la zone Europe à la page 438) • Paramètres de fuseaux horaires de la zone polaire (Paramètres de fuseaux horaires de la zone polaire à la page 438)	Fuseau horaire attribué au boîtier

Pour enregistrer les paramètres, cliquez sur **Apply** (Appliquer).

Paramètres TCP/IP du boîtier

Onglet IPv4 Settings



Onglet IPv4 Settings

Mode IP du boîtier

Lorsqu'il est activé, le paramètre **Enclosure IP Mode** (Mode IP de boîtier) assure que toutes les applications de gestion pointent vers le module Onboard Administrator actif du boîtier, en utilisant une adresse IP statique unique. Ce mode est destiné aux boîtiers dotés de modules Onboard Administrator actif et Standby. Lorsque le module Onboard Administrator en mode Standby prend le rôle du module Onboard Administrator actif, le module Onboard Administrator prend l'adresse IP du module Onboard Administrator actif précédent. Ce mode assure que l'adresse IP du mode IP de boîtier pointe de manière homogène vers le module Onboard Administrator actif.

Le paramètre **Enclosure IP Mode** (Mode IP de boîtier) requiert que le module Onboard Administrator actif dispose d'une adresse IPv4 statique ou d'une adresse IPv6 statique (IPv6 doit être activé). Le module Onboard Administrator Standby peut être configuré pour des paramètres DHCP ou d'adresse IP statique. Ce mode est facultatif et est désactivé par défaut.

Pour vous assurer que le paramètre Enclosure IP Mode n'est pas modifié lors du retrait d'un module Onboard Administrator du boîtier, ne retirez pas le module pendant qu'il est dans la phase de transition de basculement (environ six minutes après un basculement). Une fois un module retiré, pour veiller à ce que tous les paramètres sont transférés vers le module en Standby, ajoutez un module de remplacement et laissez-le en place pendant cinq minutes. Si des modules Onboard Administrator à la fois actif et en Standby sont hors tension ou retirés du boîtier en même temps, le module Onboard Administrator en Standby revient aux paramètres de réseau par défaut et toutes les adresses de réseau statiques configurées manuellement sont perdues.

REMARQUE : Cette fonction est désactivée en mode FIPS ON/DEBUG.

REMARQUE : L'activation du paramètre **Enclosure IP Mode** sur l'onglet IPv4 Settings ou IPv6 Settings active automatiquement ce mode sur les deux onglets.

Paramètres réseau de modules Onboard Administrator actif et en Standby

Le module Onboard Administrator permet de baser la configuration du réseau IPv4 sur des adresses IP attribuées dynamiquement obtenues à partir d'un serveur DHCP ou sur des adresses IP statiques que vous spécifiez manuellement. Vous choisissez la base de la configuration du réseau en sélectionnant la case d'option **DHCP** ou **Static IP Settings**. Si vous sélectionnez **DHCP**, vous pouvez activer DNS dynamique.

REMARQUE : La modification de paramètres réseau sur le module Onboard Administrator auquel vous êtes connecté peut vous déconnecter du module Onboard Administrator, auquel cas, après l'application des paramètres, vous devez vous reconnecter au module Onboard Administrator.

- **DHCP** : obtient l'adresse IP du module Onboard Administrator à partir d'un serveur DHCP.
- **Enable Dynamic DNS** : avec DHCP activé, DNS dynamique permet d'utiliser le même nom d'hôte pour le module Onboard Administrator avec le temps, bien que l'adresse IP attribuée de façon dynamique peut changer. Le nom d'hôte est inscrit avec un serveur DNS. DNS dynamique met à jour le serveur DNS avec des enregistrements nouveaux ou modifiés pour les adresses IP.

  La désactivation de DNS dynamique sur le module Onboard Administrator arrête les mises à jour du module Onboard Administrator vers le serveur DNS. Toutefois, notez que certains serveurs DHCP peuvent disposer d'une clause pour mettre à jour des serveurs DNS directement. Pour désactiver totalement les mises à jour de DNS dynamique, désactivez le service DNS dynamique au niveau du module Onboard Administrator ainsi que sur le serveur DHCP.
- **Static IP Settings** (Paramètres IP statiques) : permet de configurer manuellement des paramètres IP statiques pour le module Onboard Administrator.

ATTENTION : Lors de l'activation de DHCP pour IPv4, tous les paramètres IPv4 statiques sont perdus.

Champ	Valeur possible	Description
DNS Host Name (Nom d'hôte DNS)	Peut comprendre entre 1 et 32 caractères notamment tous les caractères alphanumériques et le tiret (-).	Le nom DNS du module Onboard Administrator. Ce paramètre s'applique aux environnements à la fois IPv4 et IPv6. Le nom d'hôte DNS peut être attribué lorsque vous utilisez des paramètres IP statiques ou DHCP. La modification du nom de DNS Onboard Administrator peut

Champ	Valeur possible	Description
		provoquer une discordance de noms d'hôte sur le certificat SSL. Vous devrez peut-être mettre à jour les informations de certificat sur le module Onboard Administrator affecté, à l'aide de l'écran Active Onboard Administrator Certificate Administration (Onglet d'informations d'administration de certificat à la page 215) ou l'écran Standby Onboard Administrator Certificate Administration (Onglet Standby Onboard Administrator Certificate Administration Information à la page 232), selon les besoins.
MAC Address (Adresse MAC)	Champ d'informations ne pouvant pas être modifié.	Adresse MAC du module Onboard Administrator.
Domain Name (Nom de domaine)	Champ d'informations ne pouvant pas être modifié.	Affiche le nom du domaine actuel de chaque module Onboard Administrator particulier
IP Address (Adresse IP)	###.###.###.### où ### est compris entre 0 et 255	Adresse IP statique du module Onboard Administrator (requise si des paramètres IP statiques sont sélectionnés).
Subnet Mask (Masque de sous-réseau)	###.###.###.### où ### est compris entre 0 et 255	Masque de sous-réseau du module Onboard Administrator (requis si des paramètres IP statiques sont sélectionnés).
Gateway (Passerelle)	###.###.###.### où ### est compris entre 0 et 255	Adresse de passerelle du module Onboard Administrator (requise si des paramètres IP statiques sont sélectionnés).
IPv4 DNS 1	###.###.###.### où ### est compris entre 0 et 255	Adresse IPv4 du premier serveur DNS IPv4.*
IPv4 DNS 2	###.###.###.### où ### est compris entre 0 et 255	Adresse IPv4 du deuxième serveur DNS IPv4.*

* L'ordre dans lequel le module Onboard Administrator utilise des serveurs DNS est décrit après cette table.

En fonction de la manière dont plusieurs serveurs DNS sont configurés, le module Onboard Administrator peut utiliser jusqu'à six serveurs DNS pour rechercher une adresse IP : deux serveurs DNS IPv4 (statiques ou affectés par DHCP, mais pas les deux) et quatre serveurs DNS IPv6 (statiques ou affectés par DHCP, ou les deux). Le module Onboard Administrator utilise des serveurs DNS dans l'ordre suivant :

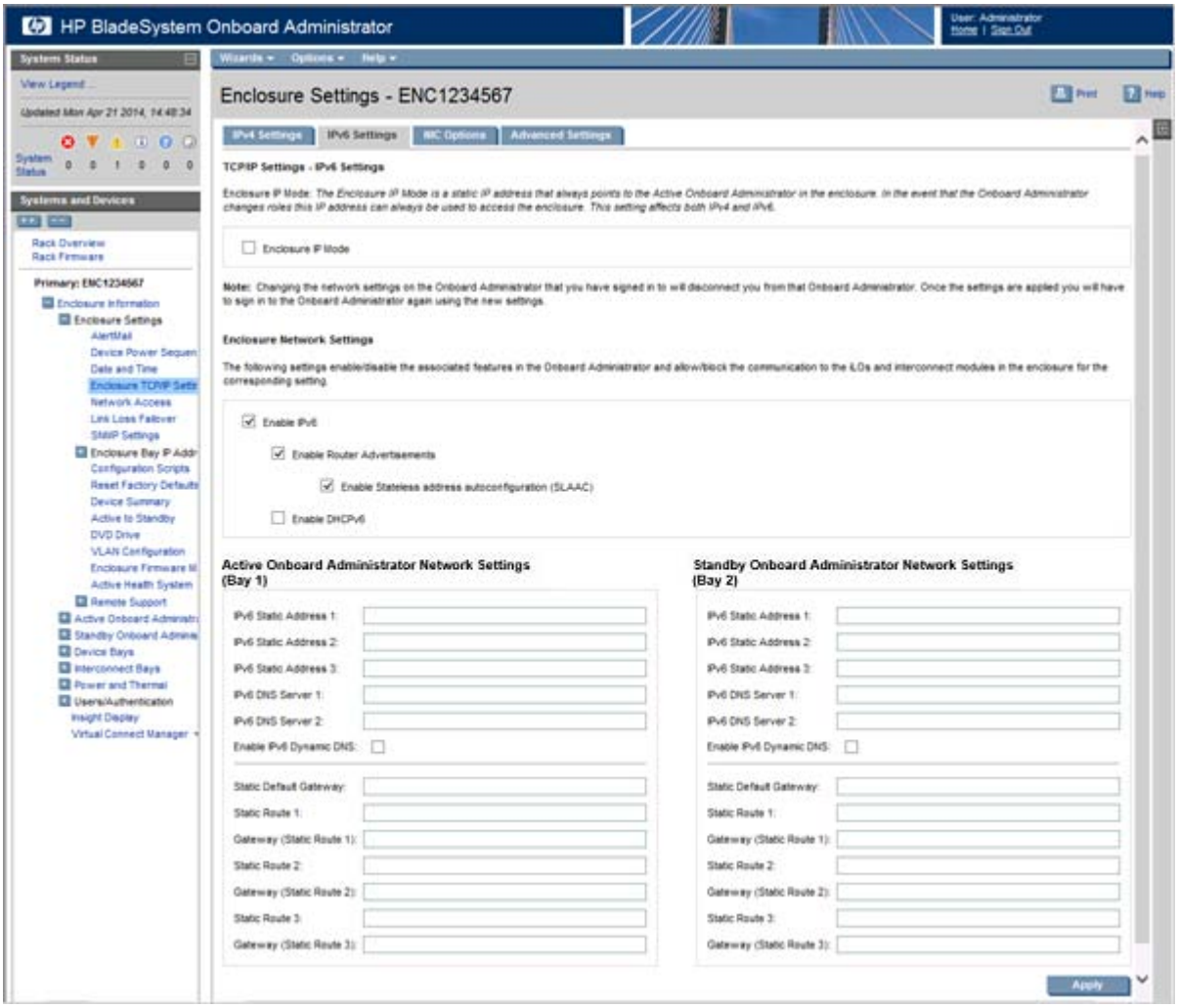
1. Serveur DNS IPv4 1 (statique)
2. Serveur DNS IPv6 1 (statique)
3. Serveur DNS IPv4 2 (statique)
4. Serveur DNS IPv6 2 (statique)
5. Serveur DNS IPv4 1 (attribué par DHCP)
6. Serveur DNS IPv6 1 (attribué par DHCP)

7. Serveur DNS IPv4 2 (attribué par DHCP)
8. Serveur DNS IPv6 2 (attribué par DHCP)

Si un des serveurs DNS dans cette liste n'est pas configuré, les serveurs DNS qui les suivent dans la liste sont déplacés vers le haut dans l'ordre, en conséquence. Par exemple, si les serveurs DNS IPv4 1 et 2 attribués par DHCP ne sont pas configurés, les deux serveurs DNS IPv6 attribués par DHCP sont déplacés en positions 5 et 6 dans la liste. Comme noté précédemment, les serveurs DNS IPv4 peuvent être statiques ou attribuée par DHCP, mais pas les deux ; par conséquent, le nombre maximum de serveurs DNS que le module Onboard Administrator peut utiliser est 6.

Pour enregistrer les nouveaux paramètres IPv4, cliquez sur **Apply** (Appliquer).

Onglet IPv6 Settings



Mode IP du boîtier

Lorsqu'il est activé, le paramètre **Enclosure IP Mode** (Mode IP de boîtier) assure que toutes les applications de gestion pointent vers le module Onboard Administrator actif du boîtier, en utilisant une adresse IP statique unique. Ce mode est destiné aux boîtiers dotés de modules Onboard Administrator actif et Standby. Lorsque le module Onboard Administrator en mode Standby prend le rôle du module Onboard Administrator actif, le premier récupère l'adresse IP du module Onboard Administrator actif précédent. Ceci assure que l'adresse IP du **mode IP de boîtier** pointe de manière homogène vers le module Onboard Administrator actif.

Le **mode IP de boîtier** requiert que le module Onboard Administrator actif dispose d'une adresse IPv4 statique ou d'une adresse IPv6 statique (IPv6 doit être activé). Le module Onboard Administrator Standby peut être configuré pour des paramètres DHCP ou d'adresse IP statique. Ce mode est facultatif et est désactivé par défaut.

Pour vous assurer que le paramètre **Enclosure IP Mode** n'est pas modifié lors du retrait d'un module Onboard Administrator du boîtier, ne retirez pas le module pendant qu'il est dans la phase de transition de basculement (environ six minutes après un basculement). Une fois un module retiré, pour veiller à ce que tous les paramètres sont transférés vers le module en Standby, ajoutez un module de remplacement et laissez-le en place pendant cinq minutes. Si des modules Onboard Administrator à la fois actif et en Standby sont hors tension ou retirés du boîtier en même temps, le module Onboard Administrator en Standby revient aux paramètres de réseau par défaut et toutes les adresses de réseau statiques configurées manuellement sont perdues.

REMARQUE : Cette fonction est désactivée en mode FIPS ON/DEBUG.

REMARQUE : L'activation du paramètre **Enclosure IP Mode** sur l'onglet IPv4 Settings ou IPv6 Settings active automatiquement ce mode sur les deux onglets.

Paramètres réseau du boîtier

IPv6 prend en charge plusieurs adresses. Vous pouvez activer n'importe quelle combinaison de paramètres réseau. Avec IPv6, SLAAC et/ou DHCPv6 activés, le module Onboard Administrator peut obtenir les adresses IP de toutes les sources sélectionnées. Il peut comporter des adresses IP attribuées automatiquement et des adresses IP statiques spécifiées par l'utilisateur. Les paramètres **Enable SLAAC**, **Enable DHCPv6** et **Enable Router Advertisements** prennent effet uniquement si IPv6 est activé.

- **Enable IPv6** (Activer IPv6) : active le protocole IPv6 pour tous les modules Onboard Administrator, les modules d'interconnexion et les modules iLO présents dans le boîtier. Lorsque cette option est activée, une adresse lien-local est automatiquement configurée.

  REMARQUE : Après avoir désactivé IPv6 en vue d'une conversion vers un environnement strictement IPv4, si l'URL d'image ISO du microprogramme sur l'onglet Enclosure Firmware Management Settings (Paramètres de gestion de microprogramme de boîtier) spécifie une clé USB ou une URL basée sur IPv6 pour un serveur Web, vous devez saisir de nouveau l'emplacement de la clé USB ou fournir une URL basée sur IPv4 pour le serveur Web. Sinon, EFM ne peut pas accéder à l'image ISO.

- **Enable Router Advertisements** (Activer annonces de routeur) : autorise les annonces de routeur IPv6 à partir du réseau de gestion externe sur le réseau interne du boîtier. Si vous désactivez ce paramètre, le module Onboard Administrator bloque les annonces de routeur IPv6 envoyées du réseau de gestion externe, les empêchant d'entrer dans le réseau de gestion interne du boîtier.
- **Enable SLAAC** (Activer SLAAC) : active les messages de configuration automatique de l'adresse sans état IPv6 pour tous les modules Onboard Administrator, les modules d'interconnexion et les modules iLO du serveur présents dans le boîtier. Cette fonction ne concerne que les adresses IPv6 globales. Lorsque IPv6 et SLAAC sont tous deux activés, le module Onboard Administrator peut obtenir jusqu'à 11 adresses IP SLAAC.
- **Enable DHCPv6** (Activer DHCPv6) : permet au module Onboard Administrator actif (et en veille, en cas de configuration adéquate) de demander une adresse IP DHCPv6. Autorise le trafic DHCPv6 sur le réseau de gestion du boîtier.

ATTENTION : Si vous désactivez IPv6 dans un environnement IPv6 uniquement, vous perdrez votre connexion à l'interface graphique du module Onboard Administrator et toutes les sessions SSH. Pour rétablir votre connexion, vous devez effectuer la configuration initiale du boîtier via les réseaux IPv4, Insight Display, ou l'interface de console série du module Onboard Administrator. Lors de la désactivation de IPv6, SLAAC ou DHCPv6, toutes les connexions qui dépendent du protocole désactivé sont fermées. Par exemple, si vous êtes connecté au module Onboard Administrator en utilisant son adresse attribuée par DHCPv6, la désactivation du paramètre DHCPv6 du boîtier résulte en la fermeture de votre session.

REMARQUE : Pour que des adresses SLAAC soient configurées avec succès, les paramètres **Enable SLAAC** et **Enable Router Advertisements** doivent être activés sur le boîtier. En outre, un routeur IPv6 doit être configuré sur le réseau de gestion du boîtier afin de fournir les adresses SLAAC via des annonces de routeur. Les cartes ILO peuvent doivent être configurées séparément pour obtenir des adresses SLAAC. Les paramètres **Enable SLAAC**, **Enable Router Advertisements** et **Enable IPv6** doivent être activés pour autoriser le trafic nécessaire sur le réseau de gestion du boîtier.

REMARQUE : Pour que des adresses DHCPv6 soient configurées avec succès, le paramètre **Enable IPv6** du boîtier doit être activé et un serveur DHCPv6 doit être configuré sur le réseau de gestion. Les cartes ILO et les modules d'interconnexion doivent être configurés séparément pour demander une adresse DHCPv6. S'ils sont configurés pour demander des adresses DHCPv6, les paramètres **Enable IPv6** et **Enable DHCPv6** doivent être activés pour autoriser le trafic nécessaire sur le réseau de gestion du boîtier.

REMARQUE : Après une réinitialisation usine, les paramètres de réseau IPv6 du boîtier (IPv6, SLAAC, DHCPv6 et annonces de routeur) sont activés par défaut.

REMARQUE : Lorsque les paramètres IPv6 Enable DHCPv6, Enable Router Advertisements ou Enable SLAAC enclosure sont désactivés sur le module Onboard Administrator, les adresses DHCPv6 ou SLAAC respectives des modules iLO du boîtier sont conservées jusqu'à leur expiration automatique en fonction de leur configuration respective. Une réinitialisation manuelle du module iLO libère immédiatement ces adresses.

Paramètres réseau de modules Onboard Administrator actif et en Standby

REMARQUE : La modification de paramètres réseau sur le module Onboard Administrator auquel vous êtes connecté peut vous déconnecter du module Onboard Administrator, auquel cas, après l'application des paramètres, vous devez vous reconnecter au module Onboard Administrator.

Champ	Valeur possible	Description
IPv6 Static Address 1 (Adresse statique 1 IPv6)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1,2]	Adresse IPv6 1 de carte réseau externe du module Onboard Administrator.
IPv6 Static Address 2 (Adresse statique 2 IPv6)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1,2]	Adresse IPv6 2 de carte réseau externe du module Onboard Administrator.
IPv6 Static Address 3 (Adresse statique 3 IPv6)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1,2]	Adresse IPv6 3 de carte réseau externe du module Onboard Administrator.

Champ	Valeur possible	Description
IPv6 DNS Server 1 (Serveur DNS IPv6 1)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128. Le préfixe est facultatif.[1]	Adresse IPv6 du premier serveur DNS IPv6 statique.[3]
IPv6 DNS Server 2 (Serveur DNS IPv6 2)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128. Le préfixe est facultatif.[1]	Adresse IPv6 du deuxième serveur DNS IPv6 statique.[3]
Enable IPv6 Dynamic DNS (Activer DNS dynamique IPv6)	Activé (case cochée) ou désactivée (case non cochée).	Permet d'utiliser un nom d'hôte pour le module Onboard Administrator qui persiste même lorsque l'adresse IP attribuée de façon dynamique peut changer. Le nom d'hôte est inscrit avec un serveur DNS. Le DNS dynamique met à jour le serveur DNS avec des enregistrements nouveaux ou modifiés pour des adresses IP.[4] La désactivation de DNS dynamique sur le module Onboard Administrator arrête les mises à jour du module Onboard Administrator vers le serveur DNS. Toutefois, notez que certains serveurs DHCP peuvent disposer d'une clause pour mettre à jour des serveurs DNS directement. Pour désactiver totalement les mises à jour de DNS dynamique, désactivez le service DNS dynamique au niveau du module Onboard Administrator ainsi que sur le serveur DHCP.
Static Default Gateway (Passerelle statique par défaut)	####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. Ne spécifiez pas de préfixe. La passerelle est supposée être accessible au sein du réseau du module Onboard Administrator.[1]	Adresse IPv6 statique de la passerelle par défaut. Ce paramètre est requis dans un environnement de réseau IPv6 configuré pour être entièrement statique. Le module Onboard Administrator peut accepter une configuration de passerelle IPv6 directement via ce paramètre et, si les annonces de routeur sont configurées, via des annonces de routeur provenant de routeurs IPv6 sur le réseau de gestion. Si des annonces de routeur fournissent une configuration de passerelle IPv6, leur configuration de passerelle remplace le paramètre de passerelle IPv6 statique. La passerelle IPv6 en cours d'utilisation par le module Onboard Administrator est affichée dans le champ Current Default Gateway (Passerelle par défaut actuelle) sur l'écran Active Onboard Administrator TCP/IP Settings (Écran TCP/IP Settings du module Onboard Administrator actif à la page 211) et l'écran Standby Onboard Administrator TCP/IP Settings.

Champ	Valeur possible	Description
Static Route 1 (Route statique 1)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1]	Ajoute une route statique IPv6 à la table de routage du module Onboard Administrator (configuration manuelle).[5] La route statique définit un chemin d'accès explicite utilisé par le module Onboard Administrator pour accéder à un réseau externe via une passerelle. Dans une configuration réseau statique, la route statique supprime la nécessité de configurer le routeur pour envoyer des informations de route via des annonces de routeur. Si les annonces de routeur sont actives dans le réseau et que la passerelle par défaut est déjà configurée, le routeur informe tous les nœuds des routes statiques disponibles, ce qui rend ainsi la configuration manuelle des routes statiques inutile. Si vous spécifiez la route statique 1, vous devez également spécifier la passerelle associée (route statique 1).
Gateway (Static Route 1) (Passerelle [Route statique 1])	####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. Ne spécifiez pas de préfixe. La passerelle doit être accessible à la fois à partir du réseau du module Onboard Administrator et du réseau externe.[1]	Adresse IPv6 de la passerelle utilisant le chemin d'accès défini par la route statique 1. Vous devez également spécifier la route statique 1.
Static Route 2 (Route statique 2)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1]	Ajoute une deuxième route statique IPv6 à la table de routage du module Onboard Administrator (configuration manuelle). Si vous spécifiez la route statique 2, vous devez également spécifier la passerelle associée (route statique 2).
Gateway (Static Route 2) (Passerelle [Route statique 2])	####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. Ne spécifiez pas de préfixe. La passerelle doit être accessible à la fois à partir du réseau du module Onboard Administrator et du réseau externe.[1]	Adresse IPv6 de la passerelle utilisant le chemin d'accès défini par la route statique 2. Vous devez également spécifier la route statique 2.
Static Route 3 (Route statique 3)	####:####:####:####:####:####:####:####/### où ### est compris entre 0 et FFFF et le préfixe /### est compris entre 1 et 128.[1]	Ajoute une troisième route statique IPv6 à la table de routage du module Onboard Administrator (configuration manuelle). Si vous spécifiez la route statique 3, vous devez également spécifier la passerelle associée (route statique 3).
Gateway (Static Route 3) (Passerelle [Route statique 3])	####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. Ne spécifiez pas de préfixe. La passerelle doit être accessible à la fois à partir du réseau du module	Adresse IPv6 de la passerelle, utilisant le chemin d'accès défini par la route statique 3. Vous devez également spécifier la route statique 3.

Champ	Valeur possible	Description
	Onboard Administrator et du réseau externe.[1]	

[1] Une version comprimée de la même adresse IPv6 est également prise en charge.
[2] Le module Onboard Administrator n'accepte pas une adresse locale de liaison comme adresse IPv6 statique.
[3] L'ordre dans lequel le module Onboard Administrator utilise des serveurs DNS est décrit après cette table.
[4] Le système DNS dynamique IPv6 nécessite qu'un serveur DNS valide (IPv4 ou IPv6) soit configuré sur le module Onboard Administrator.
[5] **Attention** : L'ajout ou la suppression d'une route statique peut entraîner la perte de connectivité pour les clients qui accèdent au module Onboard Administrator.

En fonction de la manière dont plusieurs serveurs DNS sont configurés, le module Onboard Administrator peut utiliser jusqu'à six serveurs DNS pour rechercher une adresse IP : deux serveurs DNS IPv4 (statiques ou affectés par DHCP, mais pas les deux) et quatre serveurs DNS IPv6 (statiques ou affectés par DHCP, ou les deux). Le module Onboard Administrator utilise des serveurs DNS dans l'ordre suivant :

1. Serveur DNS IPv4 1 (statique)
2. Serveur DNS IPv6 1 (statique)
3. Serveur DNS IPv4 2 (statique)
4. Serveur DNS IPv6 2 (statique)
5. Serveur DNS IPv4 1 (attribué par DHCP)
6. Serveur DNS IPv6 1 (attribué par DHCP)
7. Serveur DNS IPv4 2 (attribué par DHCP)
8. Serveur DNS IPv6 2 (attribué par DHCP)

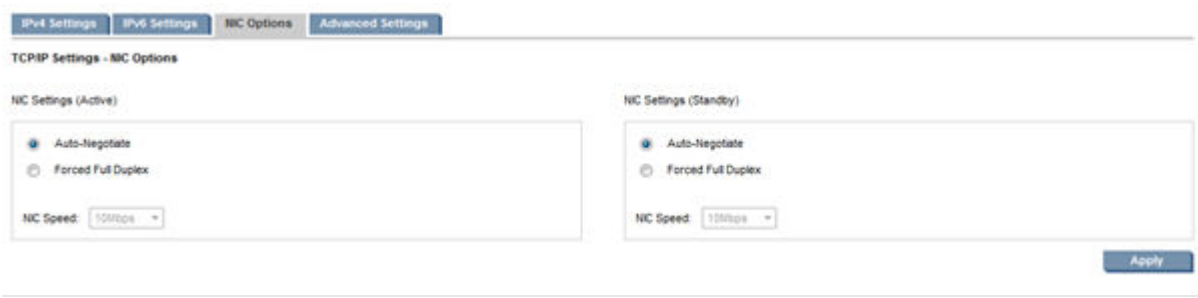
Si un des serveurs DNS dans cette liste n'est pas configuré, les serveurs DNS qui les suivent dans la liste sont déplacés vers le haut dans l'ordre, en conséquence. Par exemple, si les serveurs DNS IPv4 1 et 2 attribués par DHCP ne sont pas configurés, les deux serveurs DNS IPv6 attribués par DHCP sont déplacés en positions 5 et 6 dans la liste. Comme noté précédemment, les serveurs DNS IPv4 peuvent être statiques ou attribuée par DHCP, mais pas les deux ; par conséquent, le nombre maximum de serveurs DNS que le module Onboard Administrator peut utiliser est 6.

Pour enregistrer les nouveaux paramètres IPv6, cliquez sur **Apply** (Appliquer).

ATTENTION : Certains navigateurs comme Mozilla Firefox et Google Chrome peuvent inclure une case à cocher pour ces boîtes de dialogue contextuelles qui, si elle est sélectionnée, permettra d'éviter l'affichage de nouvelles boîtes de dialogues sur la page. N'activez pas la case à cocher sur l'une de ces boîtes de dialogue. Si vous le faites, les boîtes de dialogues resteront masquées jusqu'à ce que l'application se ferme et se recharge dans une nouvelle fenêtre de l'onglet.

REMARQUE : Lorsque vous modifiez les paramètres et cliquez sur **Apply**, un message contextuel avertit que la modification des paramètres réseau pourrait vous déconnecter du module Onboard Administrator. Lorsque vous cliquez sur **OK**, si les modifications entraînent la désactivation de certains protocoles, un autre message contextuel vous avertit que toutes les connexions utilisant ces protocoles seront fermées et que vous risquez de perdre votre session. Vous êtes invité à confirmer si vous souhaitez effectuer cette action (cliquez sur **OK** ou sur **Cancel**).

Onglet NIC Options



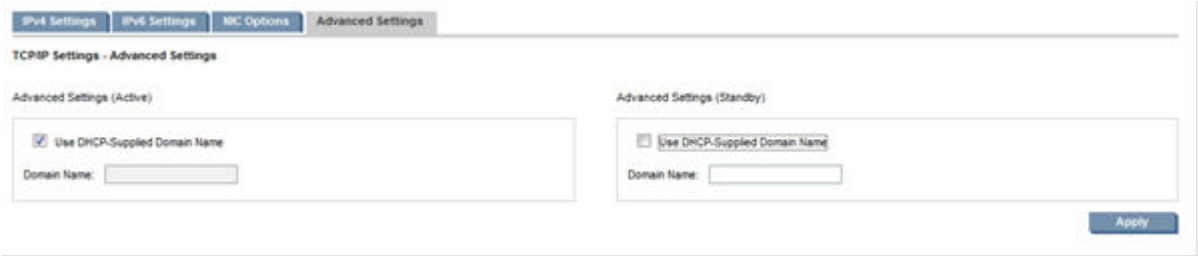
TCP/IP Settings - NIC Options (Paramètres TCP/IP - Options de carte réseau)

Paramètres NIC

- **Auto-Negotiate** (Négociation automatique) : configure automatiquement le meilleur lien. Il s'agit ici du réglage par défaut. Cette option prend en charge une vitesse de carte réseau de 10 Mo/s, 100 Mo/s ou 1 000 Mo/s. Le paramètre 1 000 Mo/s est disponible uniquement lorsque Auto-Negotiate est sélectionné.
- **Forced Full Duplex** (Bidirectionnel simultané forcé) : permet de spécifier manuellement les paramètres utilisés par la carte réseau externe lors d'une tentative d'établissement d'une liaison. Le module Onboard Administrator ne vérifie pas si les paramètres Ethernet forcés sont valides sur le réseau. Une perte de communications peut se produire si des paramètres incorrects ou incompatibles sont utilisés. Les paramètres forcés prennent effet 3 secondes après l'activation ou la désactivation des paramètres. L'option forcée prend en charge seulement des vitesses de carte réseau de 10 Mo/s ou 100 Mo/s.
- **NIC Speed** (Vitesse de carte réseau) : permet de sélectionner une vitesse de carte réseau de 10 Mo/s ou 100 Mo/s.

Pour enregistrer les nouveaux paramètres, cliquez sur **Apply** (Appliquer).

Onglet Advanced Settings

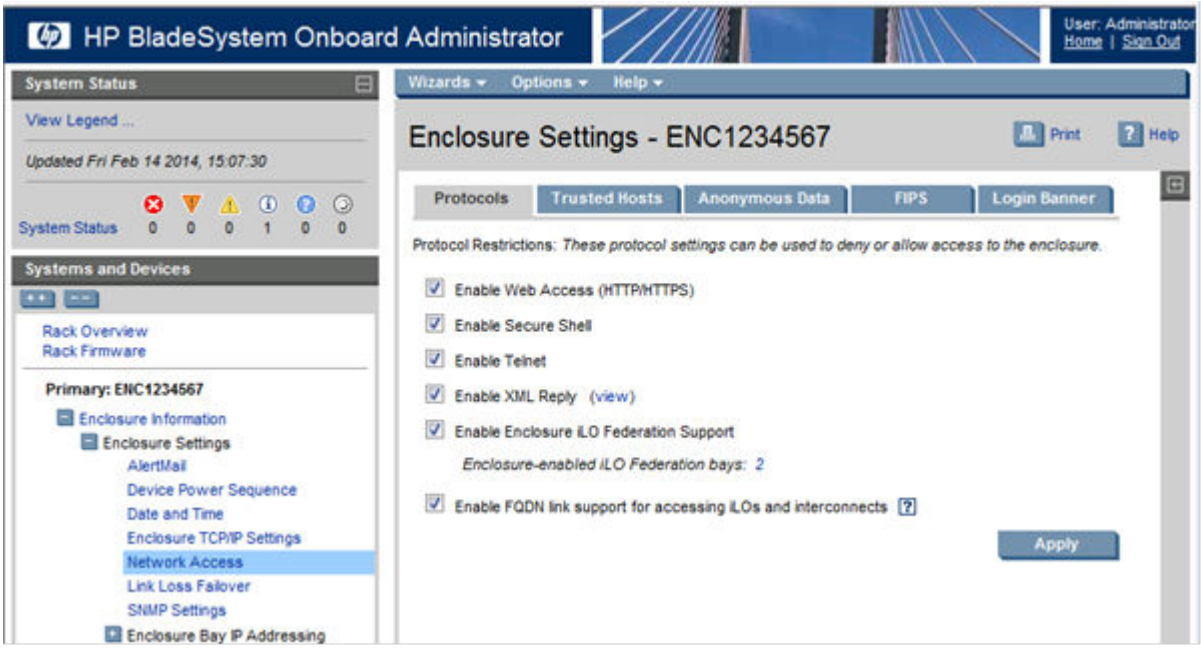


Cet écran affiche les paramètres avancés TCP/IP du boîtier actuel (Advanced Settings) pour le module Onboard Administrator actif. L'onglet Advanced Settings vous permet d'activer ou de désactiver l'option **DHCP-Supplied Domain Name** (Nom du domaine fourni par DHCP) et d'entrer les noms de domaines fournis par l'utilisateur de l'état Active (Actif) et Standby (En attente) si l'option **DHCP-Supplied Domain Name** est désactivée. Pour activer ou désactiver l'option **DHCP-Supplied Domain Name** (Nom de domaine fourni par DHCP) ou pour configurer des noms de domaine fournis par l'utilisateur, l'option DNS dynamique doit être activée. Pour activer l'option DNS dynamique, utilisez l'onglet des paramètres IPv4 (Onglet IPv4 Settings à la page 126) ou l'onglet des paramètres IPv6 (Onglet IPv6 Settings à la page 129).

Pour contourner manuellement le nom du domaine fourni par DHCP, décochez la case **Use DHCP-Supplied Domain Name** (Utiliser un nom de domaine fourni par DHCP), puis saisissez le nom du domaine. Cliquez sur **Apply** (Appliquer).

REMARQUE : Lorsque la case **Use DHCP-Supplied Domain Name** est cochée, vous ne pouvez pas modifier le champ du nom de domaine.

Accès réseau



L'administrateur peut utiliser ces paramètres pour configurer des paramètres relatifs à l'accès réseau sur le module Onboard Administrator. Ces paramètres sont spécifiques au boîtier et n'ont pas d'incidence sur les configurations réseau des lames de serveur.

Onglet Protocols

Vous pouvez sélectionner les protocoles suivants pour autoriser ou interdire l'accès au module Onboard Administrator.

- **Enable Web Access (HTTP/HTTPS)** (Activer l'accès Web) : cette case est cochée par défaut. Lorsqu'elle est désélectionnée, l'accès HTTP/HTTPS au module Onboard Administrator est désactivé. Le port 80 est utilisé pour HTTP alors que le port 443 est employé pour HTTPS.

  ATTENTION : Lorsque vous désactivez l'accès Web (HTTP/HTTPS), tous les utilisateurs liés au module Onboard Administrator via HTTP/HTTPS, y compris l'administrateur, sont désactivés.

- **Enable Secure Shell** (Activer Secure Shell) : cette case est cochée par défaut. Lorsqu'elle est désélectionnée, les connexions Secure Shell au module Onboard Administrator sont désactivées. SSH est désactivé lorsque l'authentification à deux facteurs est activée. La désélection de l'authentification à deux facteurs ne réactive pas automatiquement SSH. Pour réactiver SSH, vous devez cocher la case, puis cliquer sur **Apply** (Appliquer). Le port 22 est utilisé pour SSH.

- **Enable Telnet** (Activer Telnet) : cette case n'est pas sélectionnée par défaut. La sélection de cette case active les connexions Telnet au module Onboard Administrator. Telnet est désactivé lorsque l'authentification à deux facteurs est activée. La désélection de l'authentification à deux facteurs ne réactive pas automatiquement Telnet. Pour réactiver Telnet, vous devez cocher la case, puis cliquer sur **Apply** (Appliquer). Le port 23 est utilisé pour Telnet.

  REMARQUE : Lorsque le module Onboard Administrator fonctionne en mode FIPS ON/DEBUG, le protocole Telnet ne peut pas être utilisé.

REMARQUE : Telnet est désactivé après une réinitialisation usine ou lorsque l'authentification à deux facteurs est activée.

- **Enable XML Reply** (Activer réponse XML) : cette case est cochée par défaut. La sélection de cette case permet de partager les données XML entre le module Onboard Administrator et d'autres outils de gestion HP tels que HP Systems Insight Manager. Pour afficher les informations partagées par le module Onboard Administrator si ce protocole est activé, cliquez sur **View** (Afficher).
- **Enable Enclosure iLO Federation Support** (Activer la prise en charge du boîtier par iLO Federation) : cette case est activée par défaut. Cette case active la prise en charge du module Onboard Administrator nécessaire pour permettre la communication réseau pair à pair requise pour iLO Federation entre les cartes iLO compatibles dans le boîtier. Lorsque la prise en charge iLO Federation est activée pour le boîtier, le module Onboard Administrator actif affiche le numéro de baie de périphérique de chaque baie pour laquelle la communication réseau pair à pair est nécessaire pour l'activation de iLO Federation.

REMARQUE : L'option **Enable Enclosure iLO Federation Support** n'active que la prise en charge du module Onboard Administrator pour permettre la communication réseau pair à pair requise pour iLO Federation entre les iLO du boîtier. Pour activer intégralement iLO Federation, chaque iLO doit comporter le microprogramme approprié et être configuré pour participer dans iLO Federation. Pour plus d'informations, consultez le *Manuel de l'utilisateur de HP iLO 4* sur le site Web HP (http://www.hp.com/go/ilo/docs).

- **Enable FQDN link support for accessing iLOs and interconnects** (Activer liaison de nom de domaine complet pour accès à cartes ILO et modules d'interconnexion) : cette case à cocher n'est pas sélectionnée par défaut. La sélection de cette case entraîne l'affichage par le module Onboard Administrator d'un lien d'adresse Web basée sur le nom de domaine complet en sus des liens d'adresses Web habituelles basées sur IP pour l'accès à une carte iLO ou un module d'interconnexion à partir de l'interface Onboard Administrator. Le module Onboard Administrator interroge un serveur DNS qui effectue une recherche inversée pour le nom de domaine complet du périphérique et génère l'adresse Web basée sur FQDN (formatée en tant que nom-hôte.nom-domaine.com). Un serveur DNS IPv4 doit être configuré sur le module Onboard Administrator, et les périphériques auxquels accéder doivent être enregistrés pour la recherche inverse auprès du serveur de noms DNS. Une adresse IP du DNS doit être configurée sur le module Onboard Administrator (utilisez l'onglet Enclosure TCP/IP IPv4 Settings (Onglet IPv4 Settings à la page 126)).

  Lorsque le paramètre de nom de domaine complet est activé, les listes de liens d'URL pour tous les périphériques appropriés (cartes ILO et modules d'interconnexion) sont automatiquement actualisées et mises à jour avec les FQDN correspondants. Lorsque le paramètre de nom de domaine complet est désactivé, les liens FQDN de tous les périphériques de boîtier sont supprimés du module Onboard Administrator et par conséquent, ne sont pas affichés.

  La prise en charge de la liaison de nom de domaine complet est utile dans les environnements d'accès distant basés sur IPv6 qui dépendent d'un réseau de gestion de boîtiers basés sur IPv4 avec DNS IPv4. Elle n'est pas conçue pour les environnements IPv6 purs avec DNS IPv6.

Pour enregistrer les paramètres, cliquez sur **Apply** (Appliquer).

Onglet Trusted Hosts

Trusted Hosts

Utilisez la fonction Trusted Hosts pour restreindre l'accès au module Onboard Administrator.

Cette sous-catégorie contient une boîte de dialogue, un champ de saisie et une zone d'affichage qui, si elle est activée, est utilisée pour répertorier les adresses IP de confiance.

La case **Enable IP address access restriction** (Activer la restriction d'accès des adresses IP) n'est pas cochée par défaut. La sélection de cette case autorise uniquement les adresses IP répertoriées en tant qu'adresses fiables à se connecter au module Onboard Administrator.

⚠ **ATTENTION :** L'activation de cette restriction d'adresses IP sans avoir saisi au préalable l'adresse IP de l'utilisateur dans la liste Trusted Addresses (Adresses fiables) entraîne la déconnexion de l'utilisateur du module Onboard Administrator.

⚠ **ATTENTION :** Lors de l'utilisation de la fonction Trusted Hosts dans un environnement avec plusieurs boîtiers reliés via des câbles de liaison de boîtier, assurez-vous que tous les boîtiers liés ont les mêmes paramètres Trusted Hosts. Les boîtiers liés qui n'ont pas les mêmes paramètres Trusted Hosts peuvent autoriser un utilisateur de l'interface utilisateur Web à accéder à un boîtier protégé à partir d'un client non approuvé.

⚠ **ATTENTION :** Le document RFC 4941 décrit une extension SLAAC IPv6 qui permet à l'utilisateur de générer des adresses IPv6 temporaires de niveau global, à l'aide d'identificateurs d'interface qui changent au fil du temps. Lorsqu'un système d'exploitation qui prend en charge RFC 4941 redémarre ou que l'adresse actuelle arrive à expiration, une nouvelle adresse IPv6 temporaire est générée. Windows 7 est un exemple de système d'exploitation qui prend en charge RFC 4941.

Avec des hôtes approuvés activés, si vous accédez au module Onboard Administrator à partir d'un client hébergé sur un système d'exploitation doté d'une prise en charge de RFC 4941, un redémarrage du système d'exploitation client peut entraîner une incapacité à vous reconnecter au module Onboard Administrator. La connexion échoue parce que la nouvelle adresse IPv6 temporaire du client ne correspond pas à l'adresse IPv6 configurée pour le client dans la liste des adresses fiables. Pour éviter ce problème, désactivez la génération d'adresses IPv6 temporaires de niveau global dans le système d'exploitation ou reconfigurez l'adresse IP approuvée par l'hôte avec l'adresse IPv6 nouvellement générée du client.

Le champ Trusted Addresses est utilisé pour saisir les adresses IP de tous les hôtes fiables et autorisés à se connecter au module Onboard Administrator via les protocoles définis dans la sous-catégorie Protocol Restrictions. Ce champ est prévu pour les adresses IP uniquement. Lorsque vous spécifiez une adresse IPv6, ne spécifiez pas la longueur du préfixe.

Sous le champ Trusted Addresses (Adresses fiables) figure la zone de liste de toutes les adresses IP fiables, si de telles adresses IP sont configurées.

Pour ajouter un hôte fiable, sélectionnez son adresse IP dans le champ Trusted Addresses, puis cliquez sur **Add** (Ajouter). Vous pouvez ajouter au maximum cinq adresses fiables.

Pour supprimer un hôte fiable, sélectionnez son adresse IP dans le champ Trusted Addresses, puis cliquez sur **Remove** (Supprimer).

Pour enregistrer les paramètres, cliquez sur **Apply** (Appliquer).

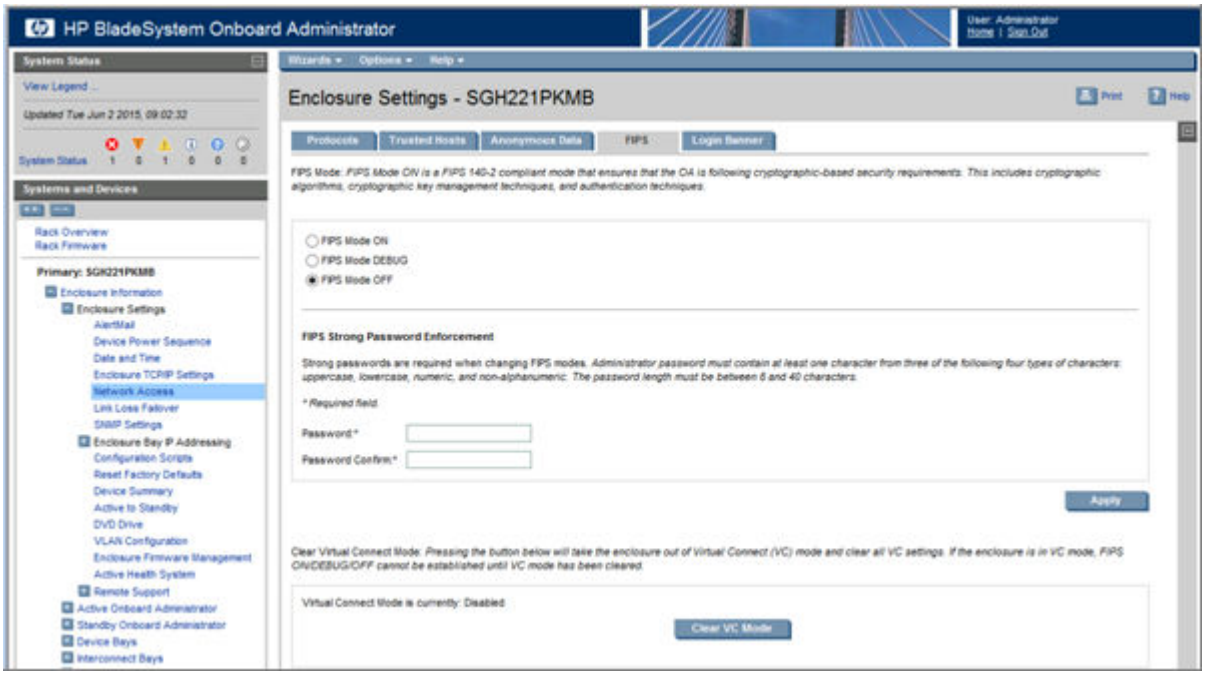
Onglet Anonymous Data

Enable Extended Data on GUI Login Page (Activer les données étendues sur la page de connexion à l'interface graphique) : cette case à cocher est sélectionnée par défaut. La désactivation de cette case à cocher désactive la fonctionnalité « + » dans la vue de topologie de la page de connexion pour ce boîtier. En outre, l'état d'intégrité du module Onboard Administrator apparaît en tant que `N/A` sur la page de connexion.

La désactivation des données étendues sur la page de connexion à l'interface graphique empêche tout utilisateur non authentifié d'afficher d'autres informations. Pour empêcher l'affichage d'autres informations pour chaque boîtier lié, vous devez désactiver cette case à cocher pour chaque boîtier.

Cliquez sur **Apply** (Appliquer) pour enregistrer les paramètres.

Onglet FIPS



Mode FIPS

REMARQUE : La modification du mode FIPS sur ON/DEBUG ou OFF ne prend pas effet sauf si le mode VC est désactivé.

REMARQUE : Lorsque le module Onboard Administrator fonctionne en mode FIPS, la longueur minimale de la clé RSA ne doit pas être inférieure à 2 048 bits, et l'algorithme de hachage de la signature doit être SHA1, SHA-224, SHA-256, SHA-384 ou SHA-512.

- **FIPS Mode OFF** : active l'utilisation d'algorithmes non approuvés par FIPS 140-2.
- **FIPS Mode ON** : met en œuvre l'utilisation du module Onboard Administrator dans un mode approuvé par FIPS 140-2. Ce paramètre prend en charge l'utilisation de chiffrements et de protocoles cryptographiques approuvés.
- **FIPS Mode DEBUG** : définit le module Onboard Administrator sur un environnement similaire au mode FIPS ON, mais avec l'option de prise en charge de débogage par HP. Le mode FIPS DEBUG possède les fonctionnalités du mode FIPS ON, mais il n'est pas considéré comme compatible FIPS en raison de l'option de débogage.

Le module Onboard Administrator redémarre une fois que toutes les modifications ont été apportées.

REMARQUE : Tous les paramètres existants sont perdus lorsque vous exécutez cette opération. Toutes les modifications apportées au paramètre du mode FIPS effectuent une opération de restauration sur les paramètres usine par défaut.

REMARQUE : En mode FIPS est sur ON/DEBUG, assurez-vous qu'un mot de passe robuste est défini.

Icônes d'état du mode FIPS

En mode FIPS ON ou DEBUG activé, l'état actuel du mode FIPS est indiqué par une icône affichée sur la barre d'en-tête du module Onboard Administrator sur les écrans de l'interface graphique. Il est

également affiché sur la page de connexion du module Onboard Administrator dans la colonne Connection de la table de boîtiers. Les icônes d'état sont décrites dans le tableau suivant :

Icône du mode FIPS	Description
	Le mode FIPS est activé (ON).
	Le mode FIPS ON a un ou plusieurs avertissements. Pour déterminer la nature de l'avertissement, placez le pointeur de la souris sur l'icône.
	Le mode FIPS DEBUG est activé.
	Le mode FIPS DEBUG a un ou plusieurs avertissements. Pour déterminer la nature de l'avertissement, placez le pointeur de la souris sur l'icône.

Exécution du mot de passe robuste FIPS

En cas de basculement entre des modes FIPS disponibles, les mots de passe robustes sont activés, la longueur minimum du mot de passe est définie sur huit caractères et un nouveau mot de passe de compte Administrateur est demandé. En outre, en cas de basculement sur le mode FIPS ON ou le mode FIPS DEBUG, le mode IP de boîtier et les protocoles Telnet, SNMPv1 et SNMPv2 sont désactivés alors que SNMPv3 est disponible.

REMARQUE : L'entrée et la sortie du mode FIPS effectuent une opération de restauration usine et verrouillent le panneau Insight Display (LCD). Si le module Onboard Administrator a été précédemment configuré avec une adresse IP statique, il prend par défaut une adresse DHCP jusqu'à ce qu'il soit reconfiguré avec une adresse IP statique. La récupération nécessite l'accès à la console série du module Onboard Administrator pour exécuter la commande `SHOW OA NETWORK` pour détecter la nouvelle adresse IP du module Onboard Administrator.

Le terme Mode FIPS est utilisé dans ce document et dans le produit pour décrire la fonction, et non son état de validation. Le processus de validation FIPS est long, c'est pourquoi toutes les versions sont validées FIPS. Pour plus d'informations sur l'état FIPS actuel de cette version ou de toute autre version du microprogramme, reportez-vous aux documents suivants :

- Programme de validation des modules cryptographiques FIPS 140-1 et FIPS 140-2 de la liste de processus (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf)
- Liste des fournisseurs FIPS 140-1 et FIPS 140-2 (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm)

Effacement du mode VC

L'effacement du mode VC supprime tous les paramètres VC du boîtier. Avant d'effacer le mode VC, mettez hors tension tous les serveurs configurés VC. Si les serveurs ne sont pas mis hors tension, ils risquent de conserver leurs paramètres VC jusqu'à leur redémarrage. Vous devez effacer le mode VC avant de modifier le paramètre du mode FIPS de OFF à ON/DEBUG ou vice versa.

Pour effacer le mode VC :

1. Cliquez sur **Clear VC Mode** (Effacer mode VC). Un écran de confirmation s'affiche, indiquant un message signifiant `Tous les serveurs doivent être mis hors tension et non configurés par Virtual Connect avant l'effacement du mode VC. Souhaitez-vous vraiment effacer le mode VC ?`
2. Cliquez sur **OK**.

Paramètres de sécurité avancés

Les exigences de sécurité FIPS peuvent changer pour un environnement particulier ou lorsque les chiffrement existants deviennent plus vulnérables aux attaques. Avec le mode FIPS ON/DEBUG, l'administrateur OA peut personnaliser des paramètres de sécurité en activant ou en désactivant des chiffrements et protocoles cryptographiques TLS sélectionnés que le module Onboard Administrator peut utiliser pour la négociation de connexions sécurisées. Les chiffrements et les protocoles pris en charge sont répertoriés dans la section « Fonctionnalités de sécurité cryptographique et valeurs par défaut » (Fonctionnalités de sécurité cryptographique et valeurs par défaut à la page 17).

ATTENTION : La désactivation d'un ou plusieurs chiffrements risque d'entraîner que certains clients perdent la connexion à l'interface utilisateur du module Onboard Administrator, selon l'ordre et la liste des chiffrements pris en charge par le client.

REMARQUE : Une fois que vous appliquez des paramètres, le service Web du module Onboard Administrator redémarre.

Pour modifier des paramètres de sécurité avancés :

1. Affichez la liste des chiffrements et protocoles cryptographiques pris en charge en cliquant sur **Edit Advanced Security Settings** (Modifier paramètres de sécurité avancés) (ce bouton est visible uniquement en Mode FIPS ON/DEBUG).
2. Pour activer ou désactiver un chiffrement ou protocole, sélectionnez ou désélectionnez la case à cocher correspondante. Vous ne pouvez pas désactiver tous les protocoles ou tous les chiffrements. Au moins un protocole et un chiffrement doivent être activés à tout moment.
3. Cliquez sur **Apply** (Appliquer).

Onglet Login Banner

Si l'option Bannière de connexion est activée, les utilisateurs du module Onboard Administrator doivent accepter le texte de la bannière pour pouvoir se connecter.

Enable Display of Banner on User Login (Activer l'affichage de la bannière lors d'une connexion utilisateur) : sélectionnez cette case à cocher pour activer l'option Login Banner (Bannière de connexion). L'acceptation du texte de la bannière de connexion donne accès à tous les systèmes connectés au module Onboard Administrator principal.

Banner Text (Texte de bannière) : la taille du champ est limitée à 1 500 caractères imprimables, les caractères % \ < > ( ) & # n'étant pas autorisés. Les espaces et retours à la ligne sont acceptés, mais il n'est pas permis d'utiliser uniquement des espaces dans ce champ de texte.

REMARQUE : La bannière de connexion accepte uniquement les caractères anglais (ASCII).

Apply (Appliquer) : cliquez pour valider le champ Banner Text (Texte de bannière). Si le champ du texte de la bannière est vide ou qu'il ne contient que des espaces, alors que la case Enable Display of Banner on User Login (Activer l'affichage de la bannière lors d'une connexion utilisateur) est cochée, vous êtes invité à désactiver cette fonction.

Link Loss Failover

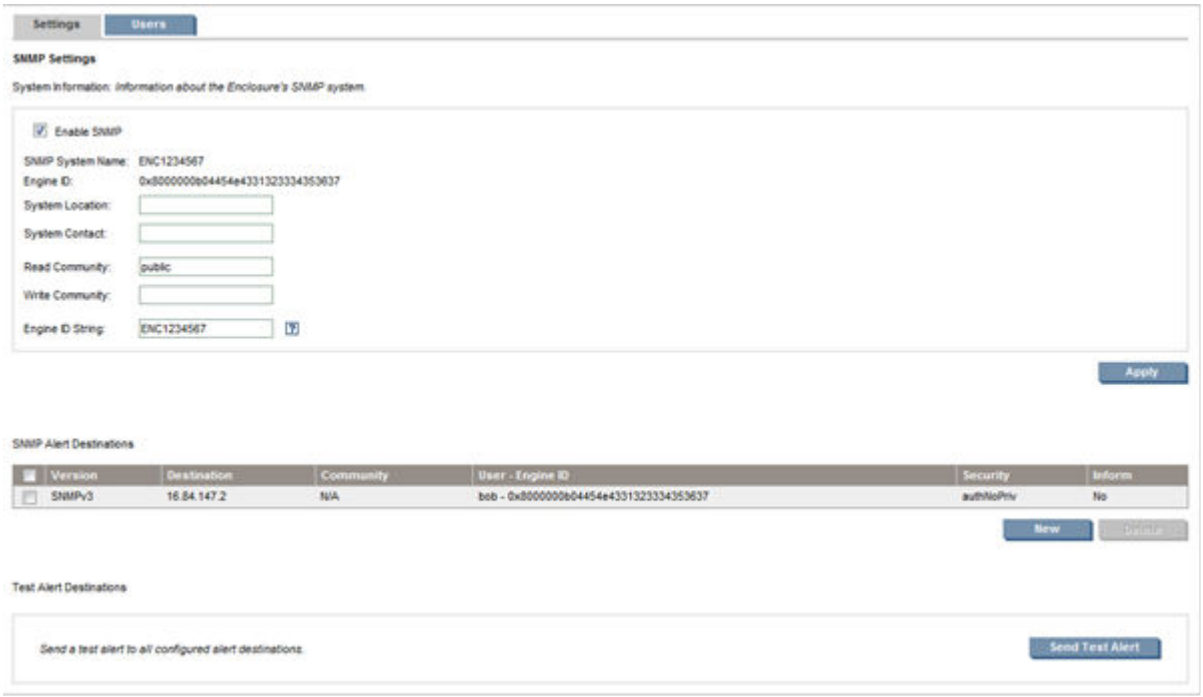
Cet écran permet de configurer le basculement automatique de redondance Onboard Administrator sur la base de l'état de la liaison réseau. Pour que le basculement sur perte de liaison fonctionne correctement, l'état de redondance du module Onboard Administrators doit être OK. Un état OK signifie que les deux modules Onboard Administrators ont la même version de microprogramme (version 2.20 ou ultérieure), et qu'ils communiquent correctement.

Enable Link Loss Failover (Activer le basculement sur perte de liaison) : cette case à cocher active ou désactive le basculement automatique sur perte de liaison.

Failover Interval (Intervalle de basculement) : l'intervalle de basculement est la durée pendant laquelle le module Onboard Administrator actif doit être sans liaison sur l'interface Ethernet externe avant que le système considère un basculement automatique. L'intervalle doit être compris entre 30 et 86400 secondes.

Cliquez sur **Apply** (Appliquer) pour enregistrer les paramètres.

Paramètres SNMP



Le protocole SNMP est utilisé pour transférer des informations de supervision entre des applications de gestion du réseau et le module HP BladeSystem Onboard Administrator. Le module Onboard Administrator prend en charge le protocole SNMP Version 1, Version 2 et Version 3, ainsi que plusieurs groupes de la MIB standard MIB-II. Des informations supplémentaires relatives à l'infrastructure du boîtier sont disponibles dans la MIB d'informations sur les racks HP. Cette MIB (CPQRACK-MIB), intégrée aux MIB Insight Management, figure sur le CD Management du ProLiant Essentials Foundation Pack.

SNMPv3 prend en charge le cryptage des données relatives à l'agent via DES ou AES128, à l'aide d'un mot de passe fourni par l'utilisateur. Un ensemble dédié d'utilisateurs SNMP est conservé, chacun avec un ensemble de mots de passe d'autorisation et d'authentification, ainsi qu'un autre ensemble de permissions par utilisateur.

L'écran SNMP Settings (Paramètres SNMP) permet d'entrer des informations système et des chaînes de communauté et de désigner les stations de gestion qui peuvent recevoir les interruptions SNMP du module Onboard Administrator. Si vous sélectionnez **Enable SNMP** (Activer SNMP), le module Onboard Administrator répond aux demandes SNMP sur le port UDP 162. Le port 162 est le port UDP standard utilisé pour envoyer et récupérer des messages SNMP.

Dans la sous-catégorie System Information (Informations sur le système), vous pouvez activer et configurer les informations relatives au système SNMP du module Onboard Administrator.

La case à cocher Enable SNMP (Activer SNMP) n'est pas sélectionnée par défaut. Lorsque cette case est sélectionnée, le module Onboard Administrator peut être interrogé pour obtenir des informations d'état et de base. Un client SNMP peut effacer l'état et des alertes SNMP uniquement lorsque vous activez la chaîne Write Community (Communauté d'écriture). Pour désactiver l'accès SNMP au module Onboard Administrator, désactivez la case **Enable SNMP**.

REMARQUE : En mode FIPS ON/DEBUG, les versions SNMPv1 et SNMPv2 sont désactivées, et vous pouvez créer uniquement des interruptions SNMPv3.

Champ	Valeur possible	Description
System Location (Emplacement du système)	0 à 20 caractères, y compris tous les caractères imprimables et les espaces	Emplacement SNMP du boîtier, utilisé généralement pour identifier l'emplacement physique ou topographique du module Onboard Administrator.
System Contact (Contact du système)	0 à 20 caractères, y compris tous les caractères imprimables et les espaces	Nom du contact du système, utilisé pour identifier la personne ou le groupe de personnes à contacter en cas de changement d'état dans le HP BladeSystem Onboard Administrator.
Read Community (Communauté de lecture)	0 à 20 caractères, y compris tous les caractères imprimables et les espaces	La chaîne Read Community (Communauté d'écriture) permet au client de lire des informations, mais pas de manipuler les alertes ou les états du HP BladeSystem Onboard Administrator via SNMPv1 ou SNMPv2. Le nom de communauté par défaut est « public » et permettra à un utilisateur de recevoir des interruptions et des alertes de notification, mais pas de modifier ou de manipuler l'état.
Write Community (Communauté d'écriture)	0 à 20 caractères, y compris tous les caractères imprimables et les espaces	La chaîne Write Community (Communauté d'écriture) permet au client de manipuler les alertes d'état du HP BladeSystem Onboard Administrator via SNMPv1 ou SNMPv2. Vous pouvez effacer des alertes et les marquer comme « viewed » (vues) ou autre à distance via leur client de supervision SNMP via les agents SNMP.
Engine ID String (Chaîne d'identifiant du moteur)	1 à 27 caractères imprimables, l'identifiant du moteur final est une chaîne hexadécimale commençant par « 0x » et résulte de cette chaîne	La chaîne d'identifiant du moteur est utilisée pour créer la valeur hexadécimale de l'identifiant du moteur. L'identifiant du moteur est combiné au nom d'utilisateur pour créer un utilisateur SNMPv3 pour chaque boîtier. Lorsque l'identifiant du moteur est unique à un boîtier, les utilisateurs ayant le même nom sur différents boîtiers sont uniques. La chaîne d'identifiant du moteur définit par défaut est le numéro de série du boîtier.

Après avoir modifié un champ dans cette sous-catégorie, pour enregistrer les modifications, cliquez sur **Apply** (Appliquer).

Ajout de destinations d'alertes SNMP

Pour supprimer une destination d'alerte SNMP actuelle, cochez la case, puis cliquez sur **Delete** (Supprimer).

Pour ajouter une nouvelle destination d'alerte SNMP, cliquez sur **New** (Nouveau). L'écran Add SNMP Alert (Ajouter une alerte SNMP) s'affiche.

Pour envoyer une interruption SNMP de test à toutes les destinations d'interruptions configurées, cliquez sur **Send Test Alert** (Envoyer alerte de test). Vous devez activer SNMP pour utiliser cette fonction.

Pour définir vos nouvelles informations d'alerte SNMP, utilisez les champs suivants.

Champ	Valeur possible	Description
Alert Destination (Destination de l'alerte)	Protocole : • udp : pour les interruptions IPv4 udp • udp6 ou udpv6 ou udpipv6 : pour les interruptions ipv6 udp • tcp : pour les interruptions IPv4 tcp (uniquement pour snmpv3) • tcp6 ou tcpv6 ou tcpipv6 : pour les interruptions ipv6 tcp (uniquement pour snmpv3) Destination : • Adresse IPv4 : ###.###.###.### où ### est compris entre 0 et 255. • Adresse Ipv6 : ####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. • Nom DNS : peut comprendre entre 1 et 64 caractères notamment tous les caractères alphanumériques et le tiret (-). Port :	Adresse IP ou nom DNS de la station de supervision. La destination de l'alerte peut être spécifiée sous le format [protocole :]destination[: port]. Le protocole et le port sont tous deux des paramètres facultatifs.

Champ	Valeur possible	Description
	Le numéro de port correspond à tout numéro de port udp/tcp valide et disponible compris dans la plage de [1;65535] (tous deux inclus). Si un port est spécifié pour une adresse IPv6, l'adresse IPv6 doit être comprise entre [...] ; par exemple, [####:####::####] : 162 pour spécifier le port 162.	
Community String (Chaîne de communauté)	0 à 20 caractères, y compris tous les caractères imprimables et les espaces	Chaîne de texte qui agit comme un mot de passe. Elle est utilisée pour authentifier les messages envoyés entre le serveur de gestion HP et le module Onboard Administrator.

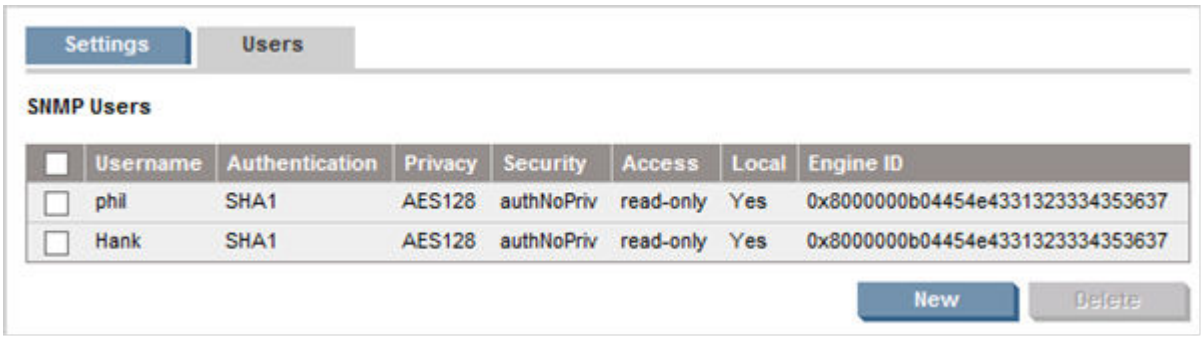
REMARQUE : En mode FIPS ON/DEBUG, les versions SNMPv1 et SNMPv2 sont désactivées, et vous pouvez créer uniquement des interruptions SNMPv3.

Pour configurer les champs suivants, cochez la case SNMPv3 :

- **User** (Utilisateur) : compte utilisateur SNMP à utiliser pour envoyer l'interruption/information. L'identifiant d'utilisateur-de moteur souhaité doit être créé avant d'ajouter la destination de l'alerte.
- **Security** (Sécurité) : niveau de sécurité utilisé pour envoyer l'interruption/information. Options de niveaux de sécurité : aucun(e) autorisation ou cryptage (noAuthNoPriv), autorisation mais pas de cryptage (authNoPriv), et autorisation et cryptage (authPriv). La valeur par défaut est authNoPriv.
- **Inform Message** (Message d'information) : si un message d'information est spécifié, l'agent attend un accusé de réception de l'application de gestion indiquant que l'interruption a été reçue. L'agent tente d'envoyer à nouveau les interruptions si aucun accusé n'a été reçu. Les alertes avec activation de message d'information doivent avoir un utilisateur à distance, qui est disponible sur une solution de gestion.

Pour ajouter l'alerte SNMP, cliquez sur **Add Alert** (Ajouter une alerte).

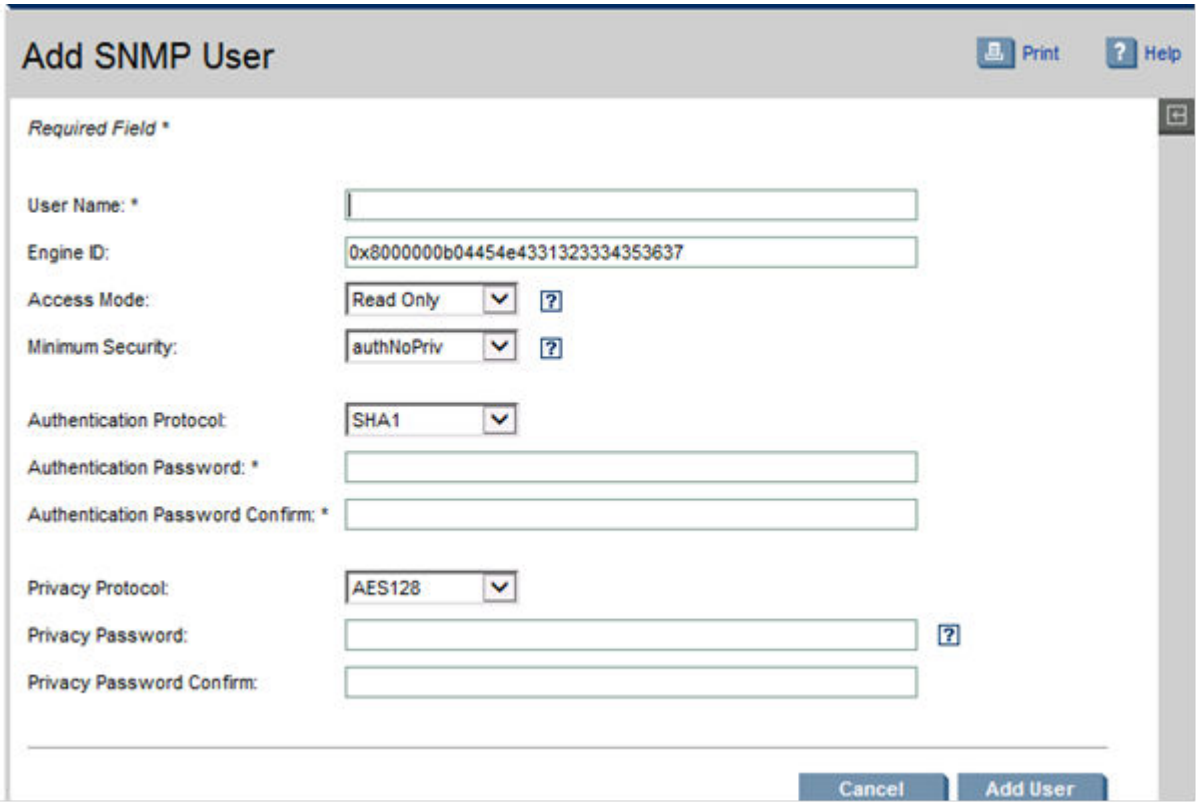
Onglet SNMP Users



Pour supprimer un utilisateur SNMP actuel, cochez la case, puis cliquez sur **Delete** (Supprimer).

Pour ajouter un nouvel utilisateur SNMP, cliquez sur **New** (Nouveau). L'écran Add SNMP User (Ajout d'utilisateur SNMP) s'affiche.

Ajout d'utilisateurs SNMP



Pour définir les informations du nouvel utilisateur SNMP, utilisez les champs suivants.

Champ	Valeur possible	Description
User Name (Nom d'utilisateur)	Chaîne unique contenant 1 à 32 caractères ; tous les caractères doivent être alphanumériques, ou bien un petit tiret ou un tiret bas et le premier caractère doit être alphabétique.	Nom de compte utilisateur utilisé pour les demandes, interruptions et informations SNMPv3. Chaque paire d'identifiant moteur/nom d'utilisateur doit être unique et ne peut pas être dupliquée.
Engine ID (Identifiant du moteur)	Doit commencer par « 0x » suivi par un nombre pair contenant jusqu'à 64 chiffres hexadécimaux.	L'identifiant du moteur est combiné au nom d'utilisateur pour créer un utilisateur SNMPv3 pour chaque boîtier. Lorsque l'identifiant du moteur est unique à un boîtier, les utilisateurs ayant le même nom sur différents boîtiers sont uniques. Définit par défaut un identifiant de moteur unique pour le boîtier. Utilisé uniquement pour créer des comptes distants utilisés avec des messages d'INFORMATION.
Access Mode (Mode d'accès)	• Lecture seule • Lecture/écriture	S'applique uniquement aux utilisateurs locaux. Indique que cet utilisateur a l'accès de lecture/d'écriture à l'arborescence OID. Si cela n'est pas spécifié, l'utilisateur aura l'accès en lecture seule.
Minimum Security (Sécurité minimale)	• noAuthNoPriv : permet les opérations non authentifiées	S'applique uniquement aux utilisateurs locaux. Niveau minimal de sécurité pour l'opération. Par défaut, l'opération doit

Champ	Valeur possible	Description
	• authNoPriv : requiert l'authentification • authPriv : requiert le cryptage	être authentifiée mais pas cryptée (authNoPriv).
Authentication Protocol (Protocole d'authentification)	• SHA1 • MD5	Utilisez l'algorithme MD5 ou SHA1, ainsi que la phrase de chiffrement pour authentifier chaque opération. MD5 ne peut pas être spécifié en mode FIPS.
Authentication Password (Mot de passe d'authentification)	De 8 à 40 caractères, comprenant tous les caractères imprimables.	Mot de passe associé à l'utilisateur.
Authentication Password Confirm (Confirmation du mot de passe d'authentification)	De 8 à 40 caractères, comprenant tous les caractères imprimables.	Mot de passe associé à l'utilisateur. Cette valeur doit correspondre à la valeur entrée dans Authentication Password (Mot de passe d'authentification).
Privacy Protocol (Protocole de confidentialité)	• AES128 • DES	Utilisez l'algorithme DES ou AES128, ainsi que la phrase de chiffrement pour crypter l'interruption. DES ne peut pas être spécifié en mode FIPS.
Privacy Password (Mot de passe de confidentialité)	Doit contenir 8 à 40 caractères imprimables.	Utilisé pour les opérations de cryptage. Si cela n'est pas spécifié, le mot de passe d'authentification est utilisé.
Privacy Password Confirm (Confirmation du mot de passe de confidentialité)	Doit contenir 8 à 40 caractères imprimables.	Utilisé pour les opérations de cryptage. Si cela n'est pas spécifié, le mot de passe d'authentification est utilisé.

Pour ajouter l'utilisateur SNMP, cliquez sur **Add User** (Ajouter utilisateur).

Adressage IP des baies de boîtiers

Les écrans EBIPA permettent de configurer des adresses IPv4 et IPv6 fixes pour les baies de boîtiers Onboard Administrator. La fonctionnalité EBIPA du module Onboard Administrator aide à configurer une adresse IP fixe basée sur le numéro de baie, qui conserve l'adresse IP d'une baie particulière, même si un périphérique est remplacé à chaud. L'interface de gestion des composants branchés sur les baies doit être définie pour le type DHCP. EBIPA ne peut être utilisé que si les périphériques sont configurés pour démarrer à partir de DHCP. Si un périphérique est configuré pour une adresse IP statique, il doit être reconfiguré manuellement pour DHCP afin de basculer sur l'adresse IP EBIPA.

REMARQUE : La documentation du module Onboard Administrator se réfère à des adresses IP EBIPA telles que des « adresses IP fixes » ou des « adresses DHCP fixes », ce qui signifie que chacune de ces adresses correspond à une adresse IP associée de façon permanente à un certain nombre de baies spécifiques indépendantes du dispositif actuel fixé à la baie.

Les baies iLO de lame de serveur et les baies de gestion de module d'interconnexion peuvent obtenir des adresses IP sur le réseau de gestion de différentes manières : adressage IP dynamique à l'aide d'un serveur DHCP externe, adressage IP statique, SLAAC via annonces de routeur (IPv6 uniquement) ou EBIPA. Si votre réseau dispose d'un service DHCP ou si vous souhaitez affecter manuellement des adresses IP statiques l'une après l'autre aux modules d'interconnexion et aux cartes iLO de lames de serveur, contournez la configuration de l'adressage IP de baies de boîtiers.

L'adressage EBIPA attribue uniquement des adresses IP DHCP fixes à l'interface de gestion pour des modules d'interconnexion et systèmes iLO de serveur sur le réseau de gestion interne au boîtier.

L'adressage EBIPA ne permet pas d'attribuer des adresses IP à d'autres périphériques sur le réseau de gestion externe au boîtier et ne peut pas être utilisé comme serveur DHCP sur le réseau de données.

La lame de serveur de iLO choisit l'adressage DHCP par défaut, obtenu via le connecteur réseau de Onboard Administrator intégré en cours. Les modules d'interconnexion disposant d'une connexion réseau de supervision à Onboard Administrator peuvent également choisir l'adresse DHCP par défaut.

REMARQUE : EBIPA applique des adresses IP uniques pour toutes les baies, même si les baies se trouvent sur un autre VLAN.

Instructions de configuration EBIPA

Cette section fournit des informations de configuration générales. Pour obtenir des informations de configuration spécifiques à IPv4 et IPv6, consultez les sections « Adressage EBIPA pour IPv4 » (Adressage EBIPA pour IPv4 à la page 150) et « Adressage EBIPA pour IPv6 » (Adressage EBIPA pour IPv6 à la page 153).

Si votre installation préfère l'attribution d'adresses IP fixes, vous pouvez spécifier des adresses fixes uniques individuellement pour chacune des baies iLO de lame de serveur et des baies de gestion du module d'interconnexion, ou vous pouvez utiliser EBIPA pour attribuer une plage d'adresses IP fixes à chaque baie de lame de serveur et de module d'interconnexion. Si vous spécifiez des adresses fixes individuellement, le masque de sous-réseau (IPv4), la passerelle, les serveurs DNS, les serveurs NTP (interconnexion IPv4) et le nom de domaine peuvent être identiques ou différents pour chaque baie. Si vous utilisez EBIPA pour attribuer une plage d'adresses fixes, vous devez spécifier la première adresse IP dans la plage et le masque de sous-réseau. Lorsque vous cliquez sur le bouton fléché vers le bas **Autofill** (Remplissage auto) de cette baie, les baies énumérées en dessous de cette dernière sont automatiquement attribuées à des adresses IP consécutives. Le masque de sous réseau, la passerelle, les serveurs DNS, les serveurs NTP et le nom de domaine sont également copiés dans chacune des baies consécutives de la liste.

Par exemple, si vous spécifiez l'adresse IPv4 16.100.226.21 pour la baie EBIPA 1 et que vous utilisez la fonctionnalité Autofill, les baies 1 à 16 sont affectées à des adresses IP consécutives dans la plage comprise entre 16.100.226.21 et 16.100.226.36. Si vous spécifiez 16.200.139.51 pour la baie d'interconnexion 3 et que vous utilisez cette fonctionnalité, les baies d'interconnexion 3 à 8 sont affectées à des adresses IP consécutives dans la plage comprise entre 16.200.139.51 et 16.200.139.56.

REMARQUE : Le bouton **Autofill** (Remplissage auto) ne remplit que tous les champs d'adresse si le champ d'adresse associé à la première adresse de la liste est sélectionné. Par exemple, le remplissage automatique de l'adresse 1 remplira les adresses 1 à 16, le remplissage automatique de l'adresse 2 remplira les adresses 2 à 16, etc.

Lors de l'utilisation du remplissage automatique, spécifiez un masque de sous-réseau IPv4 ou un préfixe de sous-réseau IPv6 qui autorise suffisamment d'adresses disponibles sur le sous-réseau associé pour remplir tous les champs d'adresse correspondant au nombre total de baies sélectionnées. Si vous spécifiez un préfixe ou un masque de sous-réseau qui ne répond pas à cette exigence, « Invalid IP Address » (Adresse IP non valide) s'affiche dans le champ d'adresse de chaque baie pour laquelle une adresse ne peut pas être générée.

Si vous utilisez des adresses IP statiques pour les processeurs de supervision, la commande `hponcfg` du module Onboard Administrator peut être utilisée pour envoyer le script RIBCL des paramètres réseau iLO à un module iLO si ce module a déjà une adresse IP. EBIPA peut être utilisé pour démarrer les adresses IP des iLO, afin que la commande `hponcfg` du module Onboard Administrator puisse être utilisée pour envoyer des scripts de configuration à ces iLO. Les modifications apportées aux paramètres de réseau iLO entraînent la réinitialisation par le système iLO de son réseau et l'interruption de toute connexion actuelle pendant quelques secondes.

Si vous possédez des lames de serveur double densité, ne configurez pas les paramètres EBIPA pour les baies de base (baie 1, 2, et ainsi de suite). Configurez les baies de côté A (1A, 2A, et ainsi de suite) et les baies de côté B (1B, 2B, et ainsi de suite). L'utilisation de la fonctionnalité Autofill attribue des adresses IP consécutives aux baies répertoriées sous la baie où vous indiquez la première adresse IP de la plage (par exemple, si vous spécifiez l'adresse IP de la baie 1A et que vous utilisez la fonctionnalité Autofill, les baies 2A, 3A, et ainsi de suite sont affectées à des adresses consécutives).

Pour configurer les baies d'interconnexion, utilisez l'onglet **Interconnect Bays**.

Pour appliquer des paramètres, cliquez sur **Apply** (Appliquer).

Les serveurs dans les baies de périphérique vont obtenir automatiquement les adresses EBIPA de baies de périphérique en quelques minutes, mais les modules commutateurs d'interconnexion doivent être redémarrés manuellement en cliquant sur le bouton **Virtual Power** (Alimentation virtuelle) dans chaque page d'informations du module d'interconnexion Onboard Administrator.

⚠ **ATTENTION :** Les modifications de configuration EBIPA sur une baie de serveur qui utilise déjà l'adressage EBIPA entraîne une réinitialisation du système iLO configuré par EBIPA. Le système iLO tente ensuite d'obtenir une adresse IP, ce qui peut entraîner une perte de connectivité pour les clients qui accèdent actuellement à la carte iLO en utilisant l'adresse précédemment configurée. Pour une baie d'interconnexion, une réinitialisation automatique n'est pas effectuée, mais les modifications de configuration peuvent entraîner une perte de connectivité pour les clients qui accèdent actuellement à la baie d'interconnexion à l'aide de l'adresse précédemment configurée.

La désactivation de l'adressage configuré par EBIPA fait en sorte que les périphériques affectés perdent leur adresse actuelle configurée par EBIPA. Les clients qui accèdent aux périphériques via cette adresse perdront la connectivité. Pour assurer l'accès du client, les périphériques doivent être configurés avec une adresse, comme au travers d'un service DHCP externe ou l'affectation d'une adresse IP statique.

Configuration de votre boîtier à l'aide EBIPA sans connexion réseau active

1. Configurez une adresse IP statique pour chaque module Onboard Administrator utilisant Insight Display et notez l'adresse IP de service OA actif sur l'écran Info du boîtier Insight Display. Reliez le PC client au port de service du boîtier (connecteur « bas » de liaison de boîtier) entre les baies OA avec un cordon de raccordement Ethernet standard. La carte réseau du PC client doit être configurée pour DHCP car elle obtiendra une adresse IP dans la plage 169.254.x.y en environ 1 minute.
2. Démarrez un navigateur Web (ou bien une session telnet ou SSH), puis sélectionnez l'adresse IP du service Onboard Administrator telle qu'elle est affichée dans la fenêtre Enclosure Info de l'écran Insight Display.
3. À l'aide du mot de passe administrateur relié au module Onboard Administrator actif, connectez-vous au module Onboard Administrator en tant qu'administrateur.
4. Activez Device Bay EBIPA avec une adresse IP fixe et activez Interconnect Bay EBIPA avec une adresse IP différente de départ.

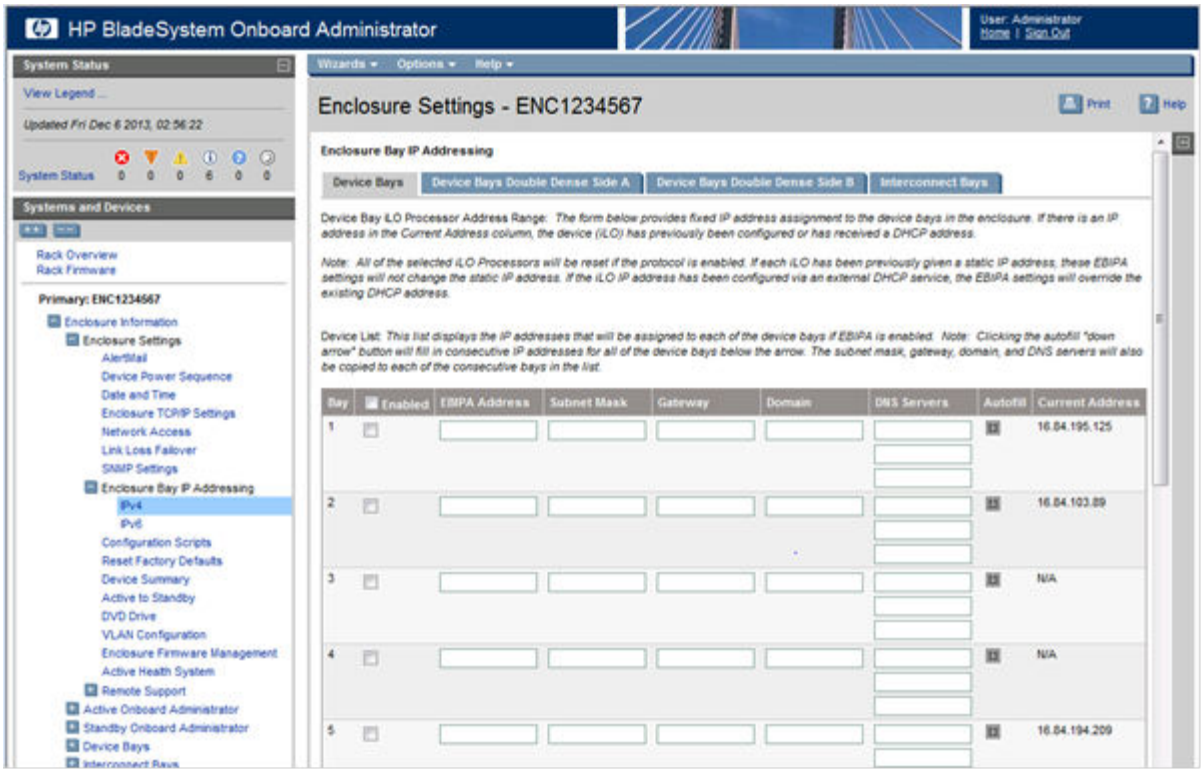
   Cliquer sur le bouton **Autofill** (Remplissage auto) crée autant d'adresses IP fixes séquentielles que nécessaire. Le masque de sous-réseau (IPv4), la passerelle, les serveurs DNS, les serveurs NTP (interconnexion IPv4) et le nom de domaine sont également copiés dans chacune des baies consécutives de la liste. Alternativement, vous pouvez attribuer manuellement des adresses IP fixes individuelles en entrant l'adresse IP souhaitée dans le champ d'adresse EBIPA pour la baie spécifique. Le masque de sous-réseau, la passerelle, les serveurs DNS, les serveurs NTP et le nom de domaine peuvent être identiques ou différents pour chaque baie.

Après avoir appliqué les paramètres, les serveurs dans les baies de périphérique vont obtenir automatiquement les adresses EBIPA de baies de périphérique en quelques minutes, mais les modules commutateurs d'interconnexion doivent être redémarrés manuellement en cliquant sur le bouton **Virtual Power** (Alimentation virtuelle) dans chaque page d'informations du module d'interconnexion Onboard Administrator.

5. Pour vérifier que les adresses iLO de lame de serveur ont été définies selon l'adresse IP de début EBIPA et la plage, utilisez la liste de périphériques Onboard Administrator.

Adressage EBIPA pour IPv4

Onglet EBIPA for IPv4 Device Bays


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
System Status
View Legend ...
Updated Fri Dec 6 2013, 02:56:22
System Status
Systems and Devices
Rack Overview
Rack Firmware
Primary: ENC1234567
Enclosure Information
Enclosure Settings
Alert Mail
Device Power Sequence
Date and Time
Enclosure TCP/IP Settings
Network Access
Link Loss Failover
SNMP Settings
Enclosure Bay IP Addressing
IPv4
IPv6
Configuration Scripts
Reset Factory Defaults
Device Summary
Active to Standby
DVD Drive
VLAN Configuration
Enclosure Firmware Management
Active Health System
Remote Support
Active Onboard Administrator
Standby Onboard Administrator
Device Bays
Interconnect Bays
Wizards
Options
Help
Enclosure Settings - ENC1234567
Print
Help
Enclosure Bay IP Addressing
Device Bays
Device Bays Double Dense Side A
Device Bays Double Dense Side B
Interconnect Bays
Device Bay iLO Processor Address Range: The form below provides fixed IP address assignment to the device bays in the enclosure. If there is an IP address in the Current Address column, the device (iLO) has previously been configured or has received a DHCP address.
Note: All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IP address, these EBIPA settings will not change the static IP address. If the iLO IP address has been configured via an external DHCP service, the EBIPA settings will override the existing DHCP address.
Device List: This list displays the IP addresses that will be assigned to each of the device bays if EBIPA is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IP addresses for all of the device bays below the arrow. The subnet mask, gateway, domain, and DNS servers will also be copied to each of the consecutive bays in the list.
Bay
Enabled
EBIPA Address
Subnet Mask
Gateway
Domain
DNS Servers
Autofill
Current Address
1
16.84.195.125
2
16.84.103.89
3
N/A
4
N/A
5
16.84.194.209

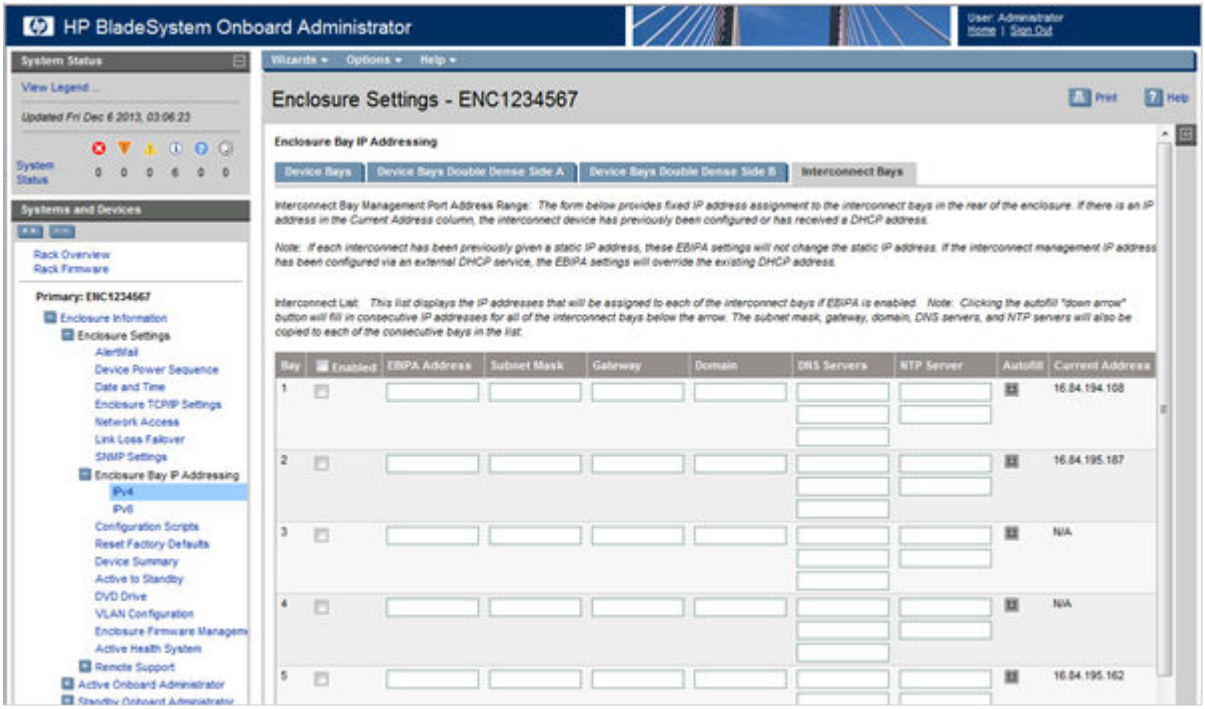
REMARQUE : N'utilisez pas la plage 169.254.x.x lors de la configuration de l'attribution des adresses EBIPA, car cette plage d'adresses réseau est réservée à l'usage du module Onboard Administrator.

Liste de périphériques

Colonne	Description
Bay (Baie)	Baie dans le boîtier du périphérique.
Enabled (Activé)	Active les paramètres EBIPA pour la baie de périphérique. Les paramètres EBIPA pour toutes les baies de périphériques peuvent être activés par la sélection de la case à cocher en regard de Enabled (Activé) dans la rangée d'en-tête ou des baies de périphériques individuelles peuvent être sélectionnées en cochant la case pour cette baie de périphérique donnée.
EBIPA Address (Adresse EBIPA)	Adresse IP fixe à affecter à la baie de périphérique. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.

Colonne	Description
Subnet Mask (Masque de sous-réseau)	Masque de sous-réseau des baies de périphérique. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Gateway (Passerelle)	Adresse IP de passerelle fixe à affecter à la baie de périphérique. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Domain (Domaine)	Nom de domaine des baies de périphérique. Les valeurs possibles sont une chaîne de caractères comprenant au maximum 64 caractères, y compris tous les caractères alphanumériques, le tiret (-) et le point (.).
DNS Servers (Serveurs DNS)	Adresses IP des serveurs DNS principal, secondaire et tertiaire. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Autofill (Remplissage auto)	Affecte des adresses IP consécutives pour les baies de périphériques sélectionnées au-dessous de la liste de périphériques. Pour attribuer les adresses IP, cliquez sur la flèche vers le bas **Autofill**. Le bouton Autofill (Remplissage auto) ne remplit que tous les champs d'adresse si le champ d'adresse associé à la première adresse de la liste est sélectionné. Par exemple, le remplissage automatique de l'adresse 1 remplira les adresses 1 à 16, le remplissage automatique de l'adresse 2 remplira les adresses 2 à 16, etc. Lors de l'utilisation du remplissage automatique, spécifiez un masque de sous-réseau IPv4 qui autorise suffisamment d'adresses disponibles sur le sous-réseau associé pour remplir tous les champs d'adresse correspondant au nombre total de baies sélectionnées. Si vous spécifiez un masque de sous-réseau qui ne répond pas à cette exigence, « Invalid IP Address » (Adresse IP non valide) s'affiche dans le champ d'adresse de chaque baie pour laquelle une adresse ne peut pas être générée.
Current Address (Adresse actuelle)	Adresse IP actuelle de la baie de périphérique.

Onglet EBIPA for IPv4 Interconnect Bays


HP BladeSystem Onboard Administrator
Enclosure Settings - ENC1234567
Enclosure Bay IP Addressing
Device Bays
Device Bays Double Dense Side A
Device Bays Double Dense Side B
Interconnect Bays

Liste d'interconnexion

REMARQUE : N'utilisez pas la plage 169.254.x.x lors de la configuration de l'attribution des adresses EBIPA, car cette plage d'adresses réseau est réservée à l'usage du module Onboard Administrator.

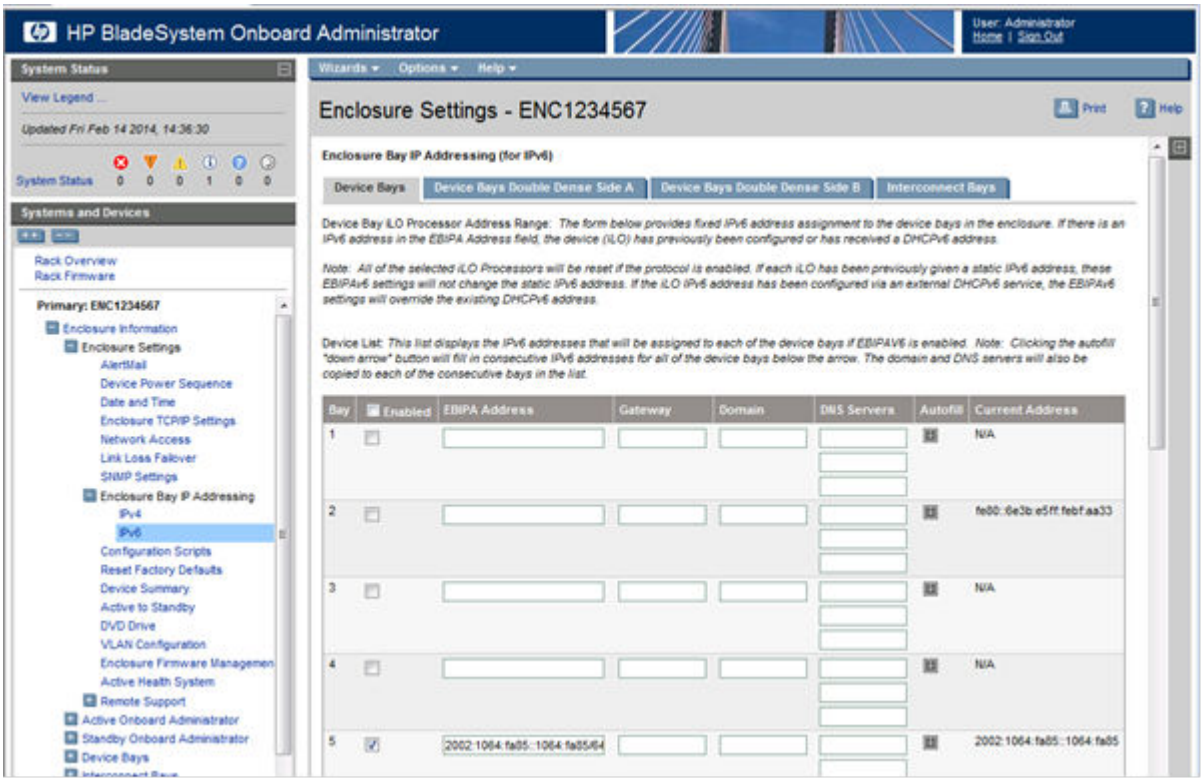
Colonne	Description
Bay (Baie)	Baie dans le boîtier du périphérique d'interconnexion.
Enabled (Activé)	Active les paramètres EBIPA pour IPv4 pour la baie d'interconnexion. Les paramètres EBIPA pour IPv4 pour toutes les baies d'interconnexion peuvent être activés par la sélection de la case à cocher en regard de Enabled (Activé) dans la rangée d'en-tête ou des baies d'interconnexion individuelles peuvent être sélectionnées en cochant la case pour cette baie d'interconnexion donnée.
EBIPA Address (Adresse EBIPA)	Adresse IP DHCP statique à affecter à la baie de périphérique.
Subnet Mask (Masque de sous-réseau)	Masque de sous-réseau des baies de périphérique. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Gateway (Passerelle)	Adresse de passerelle des baies de périphérique. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.
Domain (Domaine)	Nom de domaine des baies de périphérique. Les valeurs possibles sont une chaîne de caractères comprenant au maximum 64 caractères, y compris tous les caractères alphanumériques, le tiret (-) et le point (.).
DNS Servers (Serveurs DNS)	Adresses IPv4 des serveurs DNS principal, secondaire et tertiaire. Les valeurs possibles sont ###.###.###.### où ### est compris entre 0 et 255.

Colonne	Description
NTP Server (Serveur NTP)	Adresse IPv4 du serveur utilisée pour la synchronisation de la date et de l'heure à l'aide du protocole NTP. ###.###.###.### où ### est compris entre 0 et 255
Autofill (Remplissage auto)	Affecte des adresses IPv4 consécutives pour les baies d'interconnexion sélectionnées au-dessous de la liste d'interconnexion. Pour attribuer les adresses IP, cliquez sur la flèche vers le bas **Autofill**. Le bouton Autofill (Remplissage auto) ne remplit que tous les champs d'adresse si le champ d'adresse associé à la première adresse de la liste est sélectionné. Par exemple, le remplissage automatique de l'adresse 1 remplira les adresses 1 à 16, le remplissage automatique de l'adresse 2 remplira les adresses 2 à 16, etc. Lors de l'utilisation du remplissage automatique, spécifiez un masque de sous-réseau IPv4 qui autorise suffisamment d'adresses disponibles sur le sous-réseau associé pour remplir tous les champs d'adresse correspondant au nombre total de baies sélectionnées. Si vous spécifiez un masque de sous-réseau qui ne répond pas à cette exigence, « Invalid IP Address » (Adresse IP non valide) s'affiche dans le champ d'adresse de chaque baie pour laquelle une adresse ne peut pas être générée.
Current Address (Adresse actuelle)	Adresse IPv4 actuelle de la baie d'interconnexion.

Pour enregistrer les paramètres EBIPA pour IPv4 pour les baies d'interconnexion, cliquez sur **Apply** (Appliquer).

Adressage EBIPA pour IPv6

Onglet EBIPA for IPv6 Device Bays


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
System Status
View Legend ...
Updated Fri Feb 14 2014, 14:36:30
System Status
Systems and Devices
Rack Overview
Rack Firmware
Primary: ENC1234567
Enclosure Information
Enclosure Settings
AlertMail
Device Power Sequence
Date and Time
Enclosure TCP/IP Settings
Network Access
Link Loss Failover
SNMP Settings
Enclosure Bay IP Addressing
IPv4
IPv6
Configuration Scripts
Reset Factory Defaults
Device Summary
Active to Standby
DVD Drive
VLAN Configuration
Enclosure Firmware Management
Active Health System
Remote Support
Active Onboard Administrator
Standby Onboard Administrator
Device Bays
Wizards
Options
Help
Enclosure Settings - ENC1234567
Print
Help
Enclosure Bay IP Addressing (for IPv6)
Device Bays
Device Bays Double Dense Side A
Device Bays Double Dense Side B
Interconnect Bays
Device Bay iLO Processor Address Range: The form below provides fixed IPv6 address assignment to the device bays in the enclosure. If there is an IPv6 address in the EBIPA Address field, the device (iLO) has previously been configured or has received a DHCPv6 address.
Note: All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IPv6 address, these EBIPAv6 settings will not change the static IPv6 address. If the iLO IPv6 address has been configured via an external DHCPv6 service, the EBIPAv6 settings will override the existing DHCPv6 address.
Device List: This list displays the IPv6 addresses that will be assigned to each of the device bays if EBIPAV6 is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the device bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.
Bay
Enabled
EBIPA Address
Gateway
Domain
DNS Servers
Autofill
Current Address
1
N/A
2
fe80::6e3b:e5ff:febf:aa33
3
N/A
4
N/A
5
2002:1064:fa85::1064:fa85/64
2002:1064:fa85::1064:fa85

REMARQUE : N'utilisez pas le préfixe fe80::/10 lors de la configuration de l'attribution des adresses EBIPA : ce préfixe réseau est réservé aux adresses SLAAC de liens locaux.

REMARQUE : Pour que les adresses fixées par IPv6 EBIPA soient configurées avec succès, le paramètre **Enable IPv6** doit être activé. Pour activer ce paramètre, utilisez l'écran First Time Setup Wizard Network IPv6 Settings ou l'onglet Enclosure Settings IPv6 Settings.

Les paramètres **Enable SLAAC** (Activer SLAAC) et **Enable DHCPv6** (Activer DHCPv6) n'ont aucun effet sur la fonctionnalité IPv6 EBIPA.

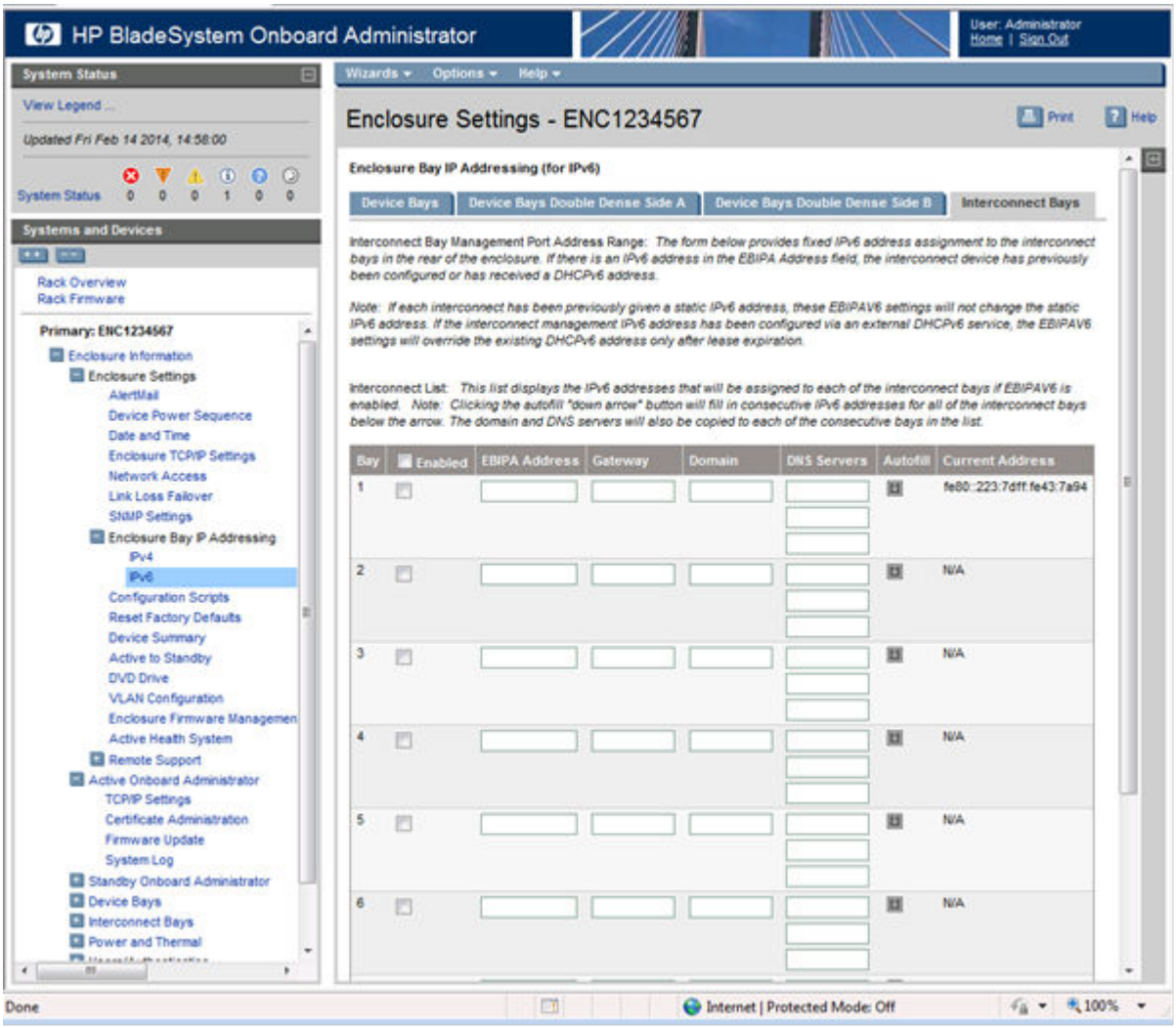
Liste de périphériques

Colonne	Description
Bay (Baie)	Baie dans le boîtier du périphérique.
Enabled (Activé)	Active les paramètres EBIPA pour la baie de périphérique. Les paramètres EBIPA pour toutes les baies de périphériques peuvent être activés par la sélection de la case à cocher en regard de Enabled (Activé) dans la rangée d'en-tête ou des baies de périphériques individuelles peuvent être sélectionnées en cochant la case pour cette baie de périphérique donnée.
EBIPA Address (Adresse EBIPA)	Adresse IPv6 fixe à affecter à la baie de périphérique. Les valeurs possibles sont ####:####:####:####:####:####:####:####/###, où #### est compris entre 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. Les plages de préfixe /### compris entre 1 et 128 ; la longueur du préfixe est obligatoire.
Gateway (Passerelle)	Adresse de passerelle IPv6 fixe à affecter à la baie de périphérique. Les valeurs possibles sont

Colonne	Description
	####:####:####:####:####:####:####:#### où #### est compris dans la plage de 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. Ne spécifiez pas de préfixe. La passerelle est supposée être accessible au sein du réseau. Si cette passerelle est spécifiée comme une adresse de liaison locale, la passerelle sera toujours configurée sur le périphérique de boîtier utilisant cette adresse. Si la passerelle est spécifiée avec tout autre type d'adresse IPv6, le module Onboard Administrator envoie des demandes de sollicitation à caractère voisin pour identifier l'adresse de liaison locale du périphérique de passerelle pour une utilisation dans le périphérique du boîtier. Si la passerelle n'existe pas ou ne répond pas aux demandes de sollicitation à caractère voisin, aucune passerelle n'est configurée.
Domain (Domaine)	Nom de domaine des baies de périphérique. Les valeurs possibles sont une chaîne de caractères comprenant au maximum 64 caractères, y compris tous les caractères alphanumériques, le tiret (-) et le point (.).
DNS Servers (Serveurs DNS)	Adresses IPv6 des serveurs DNS principal, secondaire et tertiaire. Les valeurs possibles sont ####:####:####:####:####:####:####:#### où #### est compris dans la plage de 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge.
Autofill (Remplissage auto)	Affecte des adresses IPv6 consécutives pour les baies de périphériques sélectionnées au-dessous de la liste de périphériques. Pour attribuer les adresses IP, cliquez sur la flèche vers le bas **Autofill**. Le bouton Autofill (Remplissage auto) ne remplit que tous les champs d'adresse si le champ d'adresse associé à la première adresse de la liste est sélectionné. Par exemple, le remplissage automatique de l'adresse 1 remplira les adresses 1 à 16, le remplissage automatique de l'adresse 2 remplira les adresses 2 à 16, etc. Lors de l'utilisation du remplissage automatique, spécifiez un préfixe de sous-réseau IPv6 qui autorise suffisamment d'adresses disponibles sur le sous-réseau associé pour remplir tous les champs d'adresse correspondant au nombre total de baies sélectionnées. Si vous spécifiez un préfixe ou un masque de sous-réseau qui ne répond pas à cette exigence, « Invalid IP Address » (Adresse IP non valide) s'affiche dans le champ d'adresse de chaque baie pour laquelle une adresse ne peut pas être générée.
Current Address (Adresse actuelle)	Adresse IPv6 actuelle de la baie de périphérique.

Pour enregistrer les paramètres EBIPA pour IPv6 pour les baies de périphériques, cliquez sur **Apply** (Appliquer).

Onglet EBIPA for IPv6 Interconnect Bays


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
System Status
View Legend ...
Updated Fri Feb 14 2014, 14:58:00
System Status 0 0 0 1 0 0
Systems and Devices
Rack Overview
Rack Firmware
Primary: ENC1234567
Enclosure Information
Enclosure Settings
AlertMail
Device Power Sequence
Date and Time
Enclosure TCP/IP Settings
Network Access
Link Loss Failover
SNMP Settings
Enclosure Bay IP Addressing
IPv4
IPv6
Configuration Scripts
Reset Factory Defaults
Device Summary
Active to Standby
DVD Drive
VLAN Configuration
Enclosure Firmware Management
Active Health System
Remote Support
Active Onboard Administrator
TCP/IP Settings
Certificate Administration
Firmware Update
System Log
Standby Onboard Administrator
Device Bays
Interconnect Bays
Power and Thermal
Wizards
Options
Help
Enclosure Settings - ENC1234567
Print
Help
Enclosure Bay IP Addressing (for IPv6)
Device Bays
Device Bays Double Dense Side A
Device Bays Double Dense Side B
Interconnect Bays
Interconnect Bay Management Port Address Range: The form below provides fixed IPv6 address assignment to the interconnect bays in the rear of the enclosure. If there is an IPv6 address in the EBIPA Address field, the interconnect device has previously been configured or has received a DHCPv6 address.
Note: If each interconnect has been previously given a static IPv6 address, these EBIPAV6 settings will not change the static IPv6 address. If the interconnect management IPv6 address has been configured via an external DHCPv6 service, the EBIPAV6 settings will override the existing DHCPv6 address only after lease expiration.
Interconnect List: This list displays the IPv6 addresses that will be assigned to each of the interconnect bays if EBIPAV6 is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the interconnect bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.
Bay
Enabled
EBIPA Address
Gateway
Domain
DNS Servers
Autofill
Current Address
1
fe80::223:7dff:fe43:7a94
2
N/A
3
N/A
4
N/A
5
N/A
6
N/A
Done
Internet | Protected Mode: Off
100%

Liste d'interconnexion

REMARQUE : N'utilisez pas le préfixe fe80::/10 lors de la configuration de l'attribution des adresses EBIPA : ce préfixe réseau est réservé aux adresses SLAAC de liens locaux.

Colonne	Description
Bay (Baie)	Baie dans le boîtier du périphérique d'interconnexion.
Enabled (Activé)	Active les paramètres EBIPA pour IPv6 pour la baie d'interconnexion. Les paramètres EBIPA pour IPv6 pour toutes les baies d'interconnexion peuvent être activés par la sélection de la case à cocher en regard de Enabled (Activé) dans la rangée d'en-tête ou des baies d'interconnexion individuelles peuvent être sélectionnées en cochant la case pour cette baie d'interconnexion donnée.
EBIPA Address (Adresse EBIPA)	Adresse IP IPv6 DHCP fixe à affecter à la baie d'interconnexion. Les valeurs possibles sont ####:####:####:####:####:####:####:####/###, où #### est compris entre 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. Les plages de préfixe /### compris entre 1 et 128 ; la longueur du préfixe est obligatoire.

Colonne	Description
Gateway (Passerelle)	Adresse IPv6 de passerelle fixe à affecter à la baie d'interconnexion. Les valeurs possibles sont ####:####:####:####:####:####:####:#### où #### est compris dans la plage de 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge. Ne spécifiez pas de préfixe. La passerelle est supposée être accessible au sein du réseau. Si cette passerelle est spécifiée comme une adresse de liaison locale, la passerelle sera toujours configurée sur le périphérique de boîtier utilisant cette adresse. Si la passerelle est spécifiée avec tout autre type d'adresse IPv6, le module Onboard Administrator envoie des demandes de sollicitation à caractère voisin pour identifier l'adresse de liaison locale du périphérique de passerelle pour une utilisation dans le périphérique du boîtier. Si la passerelle n'existe pas ou ne répond pas aux demandes de sollicitation à caractère voisin, aucune passerelle n'est configurée.
Domain (Domaine)	Nom de domaine des baies de périphérique. Les valeurs possibles sont une chaîne de caractères comprenant au maximum 64 caractères, y compris tous les caractères alphanumériques, le tiret (-) et le point (.).
DNS Servers (Serveurs DNS)	Adresses IPv6 des serveurs DNS principal, secondaire et tertiaire. Les valeurs possibles sont ####:####:####:####:####:####:####:####, où #### est compris entre 0 à FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge.
Autofill (Remplissage auto)	Affecte des adresses IPv6 consécutives pour les baies d'interconnexion sélectionnées au-dessous de la liste d'interconnexion. Pour attribuer les adresses IP, cliquez sur la flèche vers le bas **Autofill**. Le bouton Autofill (Remplissage auto) ne remplit que tous les champs d'adresse si le champ d'adresse associé à la première adresse de la liste est sélectionné. Par exemple, le remplissage automatique de l'adresse 1 remplira les adresses 1 à 16, le remplissage automatique de l'adresse 2 remplira les adresses 2 à 16, etc. Lors de l'utilisation du remplissage automatique, spécifiez un préfixe de sous-réseau IPv6 qui autorise suffisamment d'adresses disponibles sur le sous-réseau associé pour remplir tous les champs d'adresse correspondant au nombre total de baies sélectionnées. Si vous spécifiez un préfixe ou un masque de sous-réseau qui ne répond pas à cette exigence, « Invalid IP Address » (Adresse IP non valide) s'affiche dans le champ d'adresse de chaque baie pour laquelle une adresse ne peut pas être générée.
Current Address (Adresse actuelle)	Adresse IPv6 actuelle de la baie d'interconnexion.

Pour enregistrer les paramètres EBIPA pour IPv6 pour les baies d'interconnexion, cliquez sur **Apply** (Appliquer).

Résumé des périphériques

La section FRU Summary (Résumé des unités remplaçables sur site) présente des informations sur toutes les FRU du boîtier. Les informations présentées dans cette section peuvent aider

l'administrateur à contacter rapidement le service clientèle HP à des fins de dépannage, de réparation et de commande de pièces de remplacement.

Les informations sont organisées sous forme de tableau et réparties en sous-catégories dans la section Device Summary :

- Boîtier
- Module KVM
- Onboard Administrators
- Lames
- Mezzanines de lame
- Interconnexions
- Ventilateurs
- Alimentations

- Insight Display

Enclosure FRU Information

Part	Model	Manufacturer	Serial Number	Part Number	Spare Part Number
Enclosure	BladeSystem c7000 Enclosure	HP	ENC1234567	403320-B21	N/A
Enclosure Midplane	N/A	HP	N/A	N/A	414050-001
Onboard Administrator Tray	BladeSystem c7000 Onboard Administrator Tray	HP	OI69MK0624	N/A	416000-001
Power Input Module	HP AC Module, Single Phase	HP	N/A	N/A	413494-001

Onboard Administrator FRU Information

Bay Number	Model	Manufacturer	Serial Number	Part Number	Spare Part Number	Firmware Version	Hardware Version
1	BladeSystem c7000 DDR2 Onboard Administrator with KVM	HP	OB21BP0852	456204-B21	503826-001	3.60	B1
2	BladeSystem c7000 DDR2 Onboard Administrator with KVM	HP	OB21BP0946	456204-B21	503826-001	3.60	B1

Blade FRU Information

Bay Number	Model	Manufacturer	Serial Number	Part Number	System Board Spare Part Number
1	ProLiant BL460c G1	HP	3UV839N08G	459483R-B21	438249-001
5	ProLiant BL685c G7	HP			000000-001
7	ProLiant BL460c G6	HP	MXQ923027D	507778-B21	531221-001
9	ProLiant BL460c G1	HP	USE7507R6S	447707-B21	410299-001
10	ProLiant BL460c G1	HP	USM634043S	416654-B21	410299-001
15	ProLiant BL460c G6	HP	MXQ92707MZ	507783-B21	531221-001
16	ProLiant BL460c G1	HP	USE70638DJ	404667-B21	410299-001

Blade Mezzanine FRU Information

Bay	Mezz Slot	Model	Manufacturer	Serial Number	PCA Serial Number	Part Number	Spare Part Number
1	1	NC326m Dual Port 1Gb NIC for c-Class BladeSystem	HP	CN86MK1132	CN86MK1132	406771-B21	419330-001

Interconnect FRU Information

Bay Number	Model	Manufacturer	Serial Number	Part Number	Spare Part Number
1	HP VC Flex-10 Enet Module	HP	TW284700YT	455880-B21	456095-001
2	HP VC Flex-10 Enet Module	HP	TW28400004	455880-B21	456095-001
6	Brocade 4/24 SAN Switch for HP c-Class BladeSystem	BROCADE	CN8625701U	AE372A	411121-001

Fan FRU Information

Bay Number	Model	Part Number	Spare Part Number
1	Active Cool 200 Fan	412140-B21	413996-001
2	Active Cool 200 Fan	412140-B21	413996-001
4	Active Cool 200 Fan	412140-B21	413996-001
5	Active Cool 200 Fan	412140-B21	413996-001
6	Active Cool 200 Fan	412140-B21	413996-001
7	Active Cool 200 Fan	412140-B21	413996-001
9	Active Cool 200 Fan	412140-B21	413996-001
10	Active Cool 200 Fan	412140-B21	413996-001

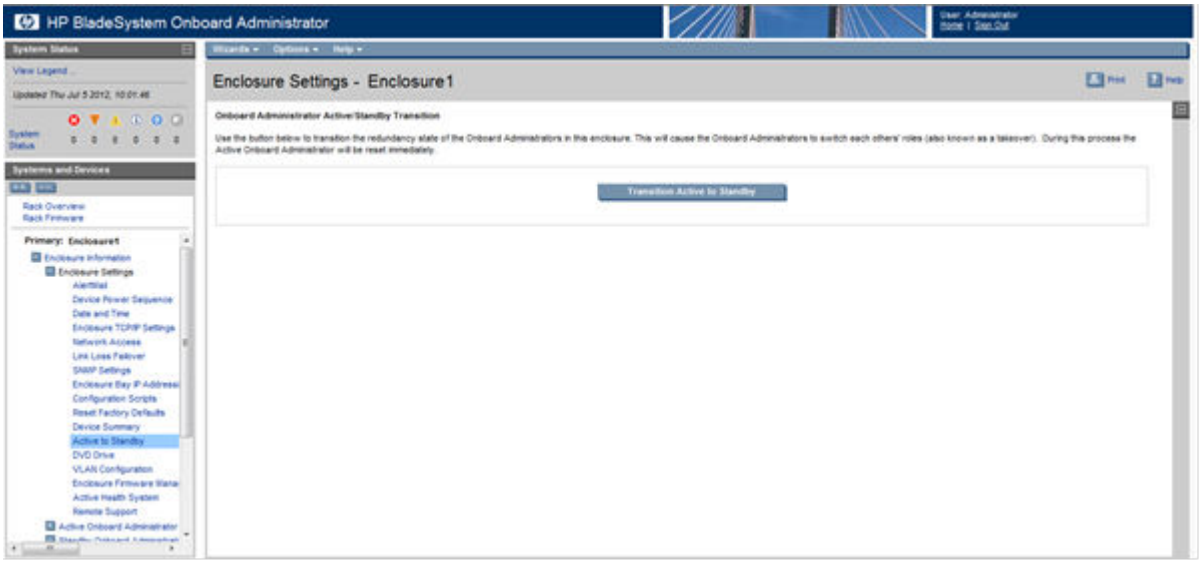
Power Supply FRU Information

Bay Number	Model	Part Number	Serial Number	Spare Part Number
1	HP BladeSystem c-Class P/S	412138-B21	5A22B0DHLU20FR	411099-001
2	HP BladeSystem c-Class P/S	412138-B21	5A22B0EHLV74LW	411099-001
3	HP BladeSystem c-Class P/S	412138-B21	5A22B0DHLTT4G3	411099-001
4	HP BladeSystem c-Class P/S	412138-B21	5A22B0EHLVR0AB	411099-001
5	HP BladeSystem c-Class P/S	412138-B21	5A22B0EHLUG0AD	411099-001
6	HP BladeSystem c-Class P/S	412138-B21	5A22B0DHLTT34Q	411099-001

Insight Display FRU Information

Model	Spare Part Number	Manufacturer	Firmware Version
BladeSystem c7000 LCD	415839-001	HP	2.2.2

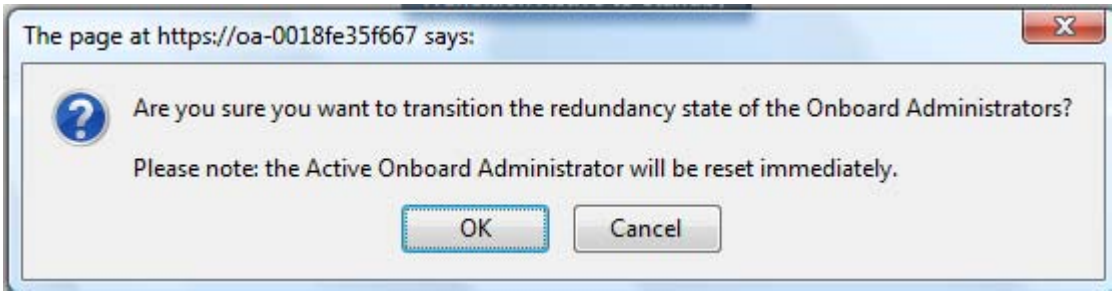
Actif à Standby



Lorsqu'un second module HP BladeSystem Onboard Administrator est installé, l'élément de menu **Active to Standby** (Actif à mode En veille) apparaît sous l'élément du menu d'arborescence **Enclosure Settings** (Paramètres du boîtier), et les deux modules Onboard Administrator sont visibles dans le menu d'arborescence et dans la vue du boîtier sous l'onglet Status (État).

Si plusieurs modules Onboard Administrator sont installés dans le boîtier, vous pouvez modifier manuellement celui actif. Cette fonction peut s'avérer utile lorsque vous dépannez le module Onboard Administrator, ou si un second module Onboard Administrator a été installé avec une version de microprogramme plus ancienne (et si le basculement automatique est désactivé).

Pour réaliser une transition, cliquez sur **Transition Active to Standby** pour forcer la modification. Un écran de confirmation s'affiche, confirmant la transition et vous recommandant de fermer votre navigateur si vous êtes connecté au module Active Onboard Administrator. Cliquez sur **OK** pour continuer, ou sur **Cancel** (Annuler) pour quitter sans apporter de modification.


The page at https://oa-0018fe35f667 says:
Are you sure you want to transition the redundancy state of the Onboard Administrators?
Please note: the Active Onboard Administrator will be reset immediately.
OK
Cancel

Vous pouvez également effectuer une transition à l'aide de la commande `FORCE TAKEOVER` à partir de l'interface CLI de Onboard Administrator.

Le temps de transition du mode actif au mode Standby et inversement varie en fonction de la configuration, du remplissage du boîtier et de divers autres facteurs. Le retrait du module Onboard Administrator précédemment actif au début du processus de transition oblige le temps de transition du passage de l'état Standby à l'état Actif à augmenter.

Lecteur de DVD

Cet écran permet de connecter plusieurs lames de serveur du boîtier à la ressource de DVD partagée, de lancer la console distante iLO et d'utiliser des commandes d'alimentation virtuelle sur

les lames de serveur sélectionnées. Les informations sur cette page sont actuelles à l'heure du dernier téléchargement. Pour visualiser des informations mises à jour, cliquez sur **Refresh** (Actualiser).

REMARQUE : Les performances de la fonctionnalité de support virtuel iLO Integrity et HP c-Class BladeSystem ProLiant seront limitées par l'activité et le nombre de sessions simultanées de support virtuel iLO et la charge de travail Onboard Administrator. Les fonctionnalités Enclosure Firmware Management et de DVD de boîtier Onboard Administrator utilisent également la fonction de support virtuel iLO et auront des restrictions de performances similaires. Pour éviter les problèmes de délai d'attente de support, HP recommande de limiter le nombre de sessions simultanées. Si des problèmes de délai d'attente sont rencontrés au cours d'une installation de système d'exploitation ou de mises à jour de microprogramme, réduisez le nombre de sessions de support virtuel en cours et redémarrez l'opération.

Colonne	Description ou action
Case à cocher	Pour appliquer la fonction Virtual Power, One Time Boot ou DVD, sélectionnez les baies.
Bay (Baie)	Ce champ affiche le numéro de baie de périphérique de la lame dans le boîtier.
Power State (État de l'alimentation)	État de l'alimentation de la lame de serveur. Les valeurs possibles sont On (Activé) et Off (Désactivé).
Remote Console (Console distante)	Pour lancer la console distante iLO, sélectionnez **Integrated Remote Console (IE)** (Console distante intégrée) (IE) ou **Remote Console (Java)** (Console distante) (Java), puis cliquez sur **Launch** (Lancer).
iLO DVD Status (État de DVD iLO)	Ce champ indique si la lame de serveur dispose d'une connexion Virtual Media. Les valeurs possibles sont Connected (Connecté), Disconnected (Déconnecté) ou Unknown (Inconnu). Un état Incompatible Firmware (Microprogramme incompatible) indique que la fonctionnalité DVD n'est pas prise en charge avec le microprogramme iLO installé sur le périphérique. Un état Unknown (Inconnu) indique la présence d'un problème de connectivité iLO.
Device or Image URL (URL d'image ou périphérique)	Ce champ affiche la connexion Virtual Media actuelle de la lame. Les valeurs possibles sont : • Standby OA DVD • Enclosure Firmware Management • Virtual Media Applet is connected • Feature not supported on Integrity iLO version x.xx • SSH is disabled on this blade's iLO processor • Upgrade ProLiant iLO 2 version x.xx to 1.30 or higher • Enclosure DVD • Tray Open or No Media • iLO has no IP address

Virtual Power

Le menu déroulant Virtual Power active une pression momentanée ou une pression et un maintien du bouton d'alimentation, ou un démarrage à froid des lames de serveur sélectionnées.

Bouton	Description
Momentary Press (Pression momentanée)	Ce bouton réplique une pression momentanée physique du bouton d'alimentation sur la lame de serveur. Un clic sur ce bouton met sous ou hors tension la lame de serveur de manière ordonnée.
Press and Hold (Appuyer et maintenir enfoncé)	Ce bouton réplique une pression physique et un maintien enfoncé du bouton d'alimentation sur la lame de serveur. Un clic sur ce bouton force la mise hors tension de la lame de serveur sans mise hors tension préalable du système d'exploitation. Cette option n'est pas disponible lorsque la lame de serveur est hors tension.
Cold Boot (Démarrage à froid)	Un clic sur ce bouton supprime immédiatement l'alimentation du système. Cette commande s'applique uniquement aux lames de serveur qui sont sous tension. L'envoi d'une commande Cold Boot (Redémarrage à froid) vers une lame de serveur hors tension entraîne la mise sous tension de cette lame.

One Time Boot

Option	Description
Diskette Drive (A:) (Lecteur de disquette (A:))	Force la lame de serveur à redémarrer à partir du lecteur de disquette. Vérifiez que le lecteur de disquette est connecté à la lame de serveur avant de sélectionner cette option.
CD-ROM	Force la lame de serveur à redémarrer à partir du lecteur de CD-ROM. Vérifiez que le lecteur de CD-ROM est connecté à la lame de serveur avant de sélectionner cette option.
Hard Drive C: (Disque dur C:)	Force la lame de serveur à redémarrer à partir du disque dur.
RBSU	Force la lame de serveur à démarrer sur l'outil ROM-Based Setup Utility.
PXE NIC	Force la lame de serveur à démarrer à partir de la carte réseau PXE.

DVD

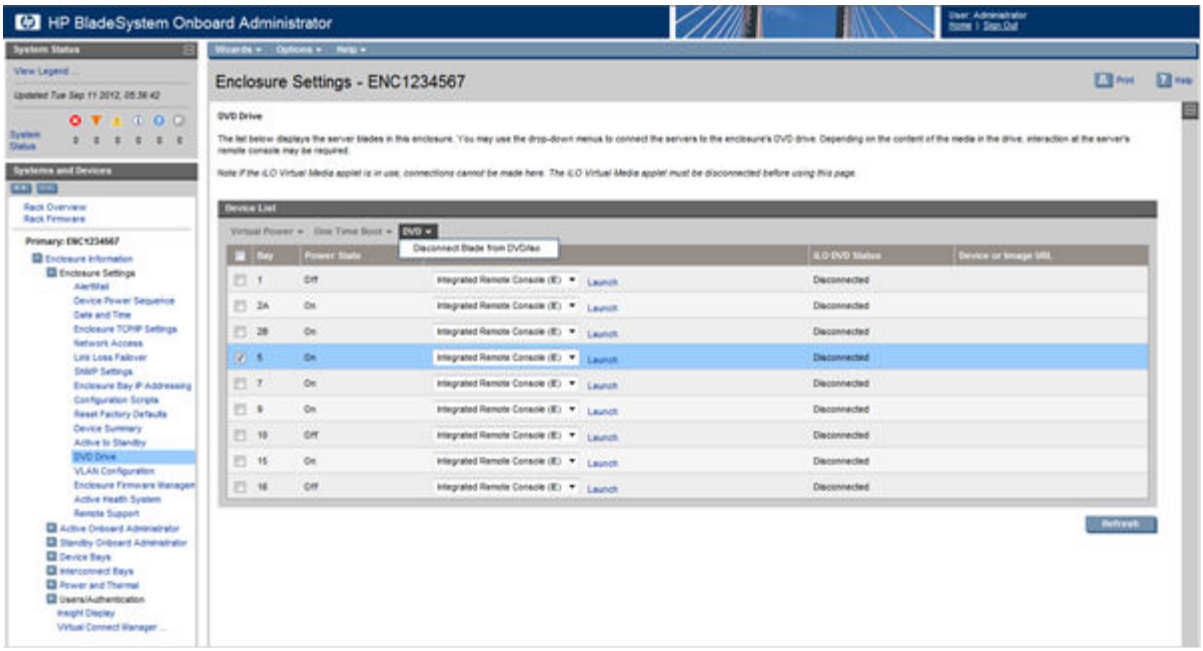
Le menu DVD permet de connecter ou déconnecter le lecteur de DVD partagé en sélectionnant Connect to Enclosure DVD (Connecter au DVD du boîtier) ou Disconnect DVD Hardware (Déconnecter matériel DVD). Vous pouvez connecter le lecteur de DVD partagé à plusieurs lames de serveur. Une fois l'unité de DVD partagée connectée, vous pouvez utiliser le menu Virtual Power pour redémarrer les lames de serveur sélectionnées dans la liste. Si plusieurs disques de support sont requis pour une installation, vous pouvez avoir à effectuer une déconnexion, puis une reconnexion pour chaque serveur lors de l'insertion du nouveau disque de support dans l'unité de DVD.

Lorsqu'une clé USB est détectée sur le port USB du module Onboard Administrator actif et que des images ISO sont présentes, ces éléments apparaissent dans le menu DVD. Sélectionnez les lames de serveur vers lesquelles déployer une image ISO, puis sélectionnez l'image ISO dans le menu. L'image ISO est déployée.

Installation et configuration interactives du lecteur de DVD/CD-ROM

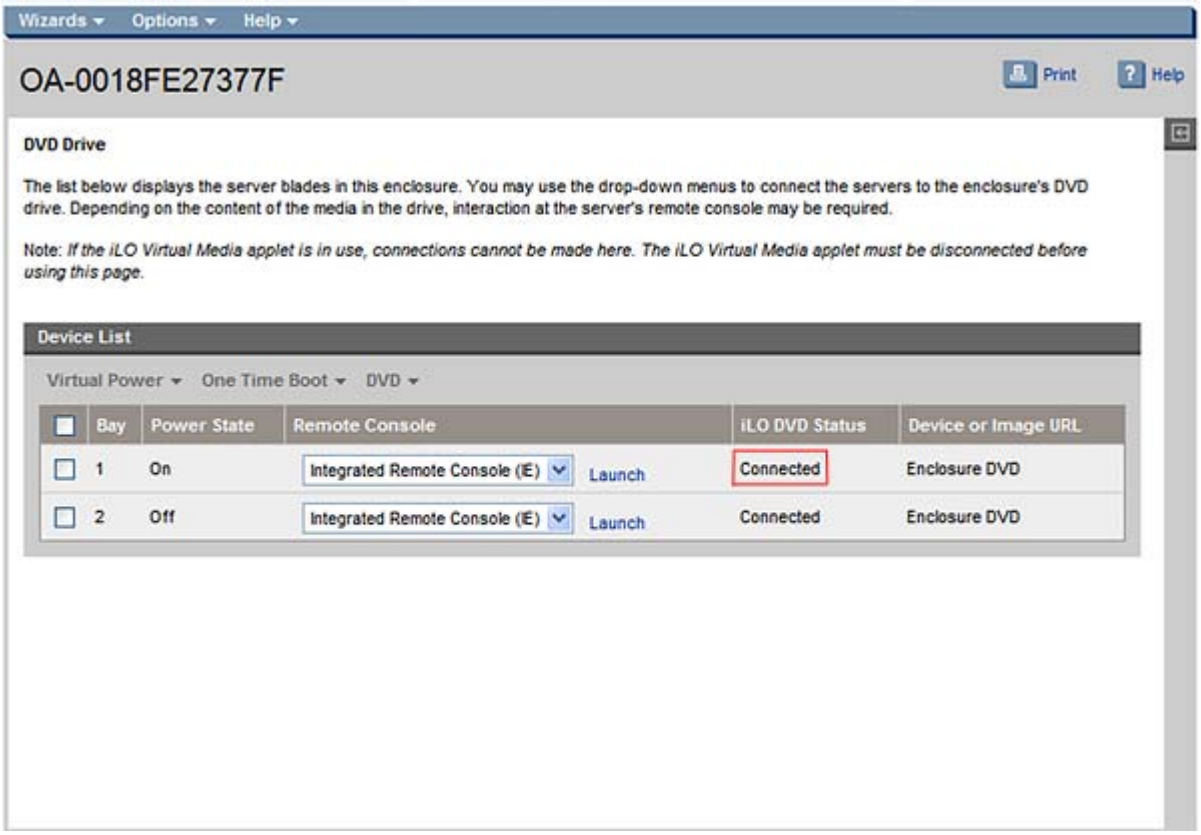
Vous pouvez installer et configurer une application logicielle ou un système d'exploitation de lame de manière interactive.

Les lames peuvent accéder au support dans le lecteur de DVD, tout d'abord en connectant la lame au lecteur de DVD, puis en navigant vers la page DVD Drive (Lecteur de DVD) ou Device Bay Summary (Résumé de baies de périphérique). Pour accéder au support dans le lecteur de DVD, insérez un disque dans le lecteur, sélectionnez le menu DVD, puis cliquez sur **Connect to Enclosure DVD** (Connecter au DVD du boîtier).



Une fois le disque inséré dans le lecteur de DVD, vous pouvez mettre sous tension ou redémarrer la lame via les options de menu correspondantes du lecteur de DVD sur la page de mappage de la liste de périphériques du module Onboard Administrator. Pour démarrer une session de console distante iLO et afficher la console de lame sélectionnée, cliquez sur **Launch** (Lancer). Les performances peuvent varier lorsque le nombre de lames augmente.

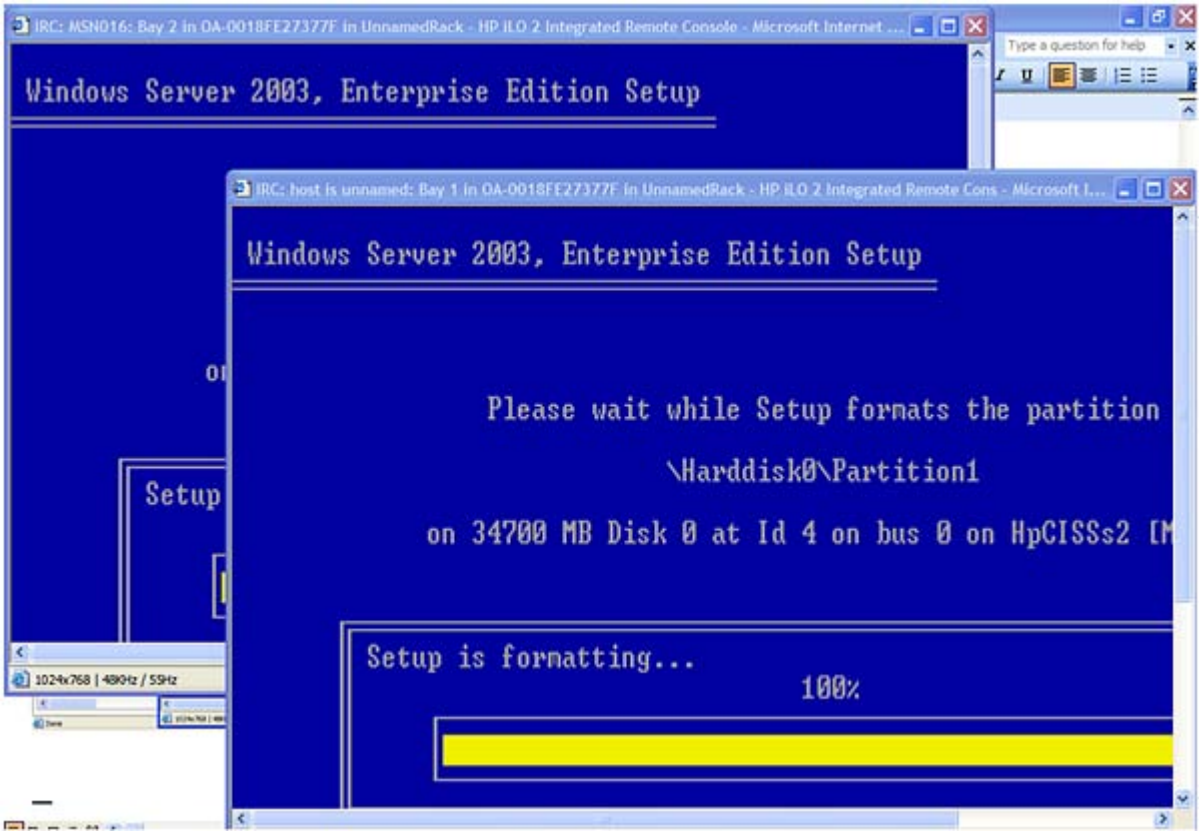
Pour plus d'informations sur l'utilisation de la console distante iLO, consultez le manuel de l'utilisateur iLO.


Wizards
Options
Help
OA-0018FE27377F
Print
Help
DVD Drive
The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.
Note: If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.
Device List
Virtual Power
One Time Boot
DVD
Bay
Power State
Remote Console
iLO DVD Status
Device or Image URL
1
On
Integrated Remote Console (IE)
Launch
Connected
Enclosure DVD
2
Off
Integrated Remote Console (IE)
Launch
Connected
Enclosure DVD

Si un CD d'installation Windows® est placé dans le lecteur de DVD, l'utilisateur peut employer l'affichage de la console distante intégrée comme illustré ci-dessous.

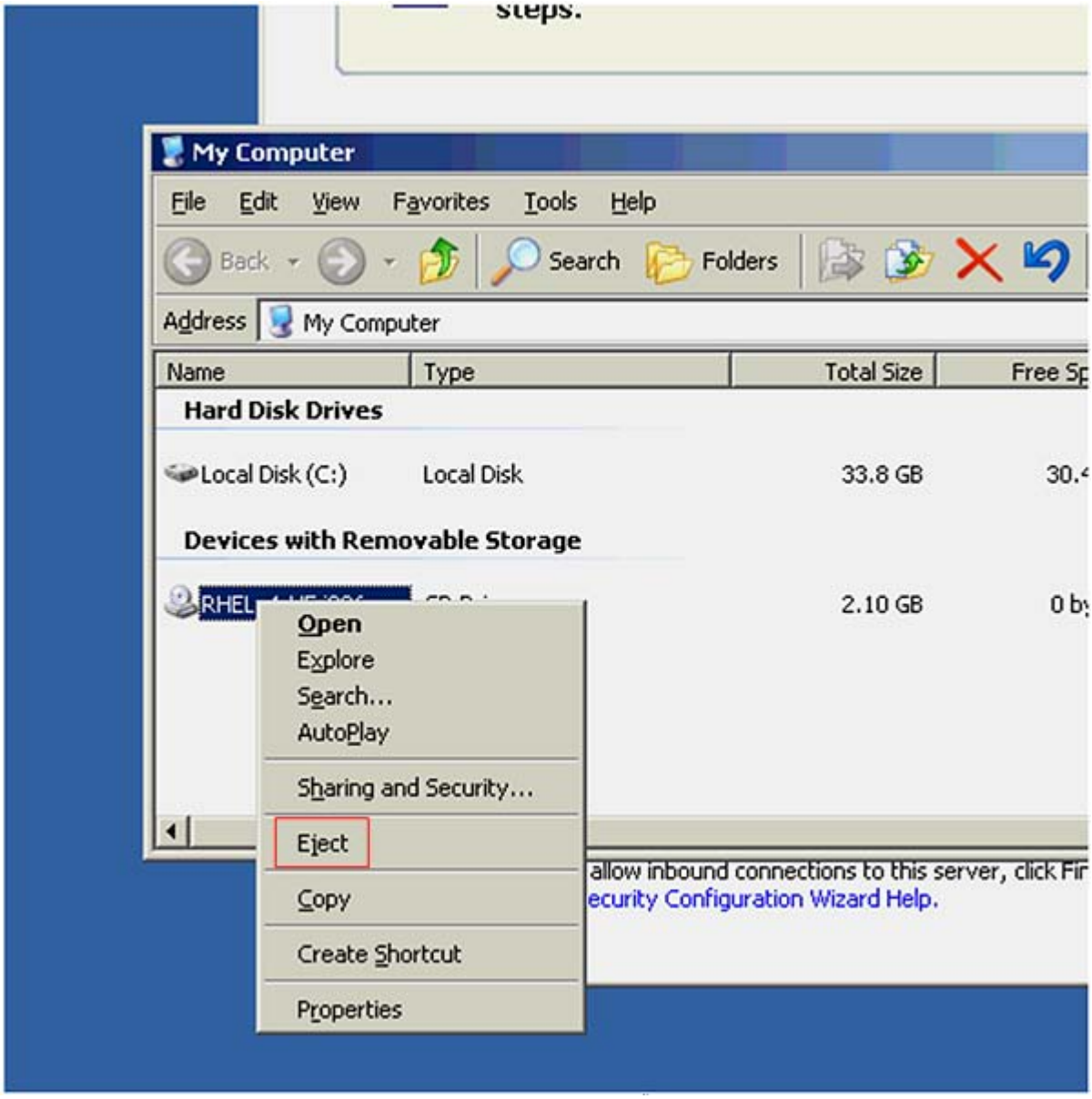
Windows Server 2003, Enterprise Edition Setup
Welcome to Setup.
This portion of the Setup program prepares Microsoft(R) Windows(R) to run on your computer.
• To set up Windows now, press ENTER.
• To repair a Windows installation using Recovery Console, press R.
• To quit Setup without installing Windows, press F3.

Installation de Windows Server® 2003 sur la lame.


Windows Server 2003, Enterprise Edition Setup
Windows Server 2003, Enterprise Edition Setup
Please wait while Setup formats the partition
\Harddisk0\Partition1
on 34700 MB Disk 0 at Id 4 on bus 0 on HpCISSs2
Setup is formatting...
100%
Setup

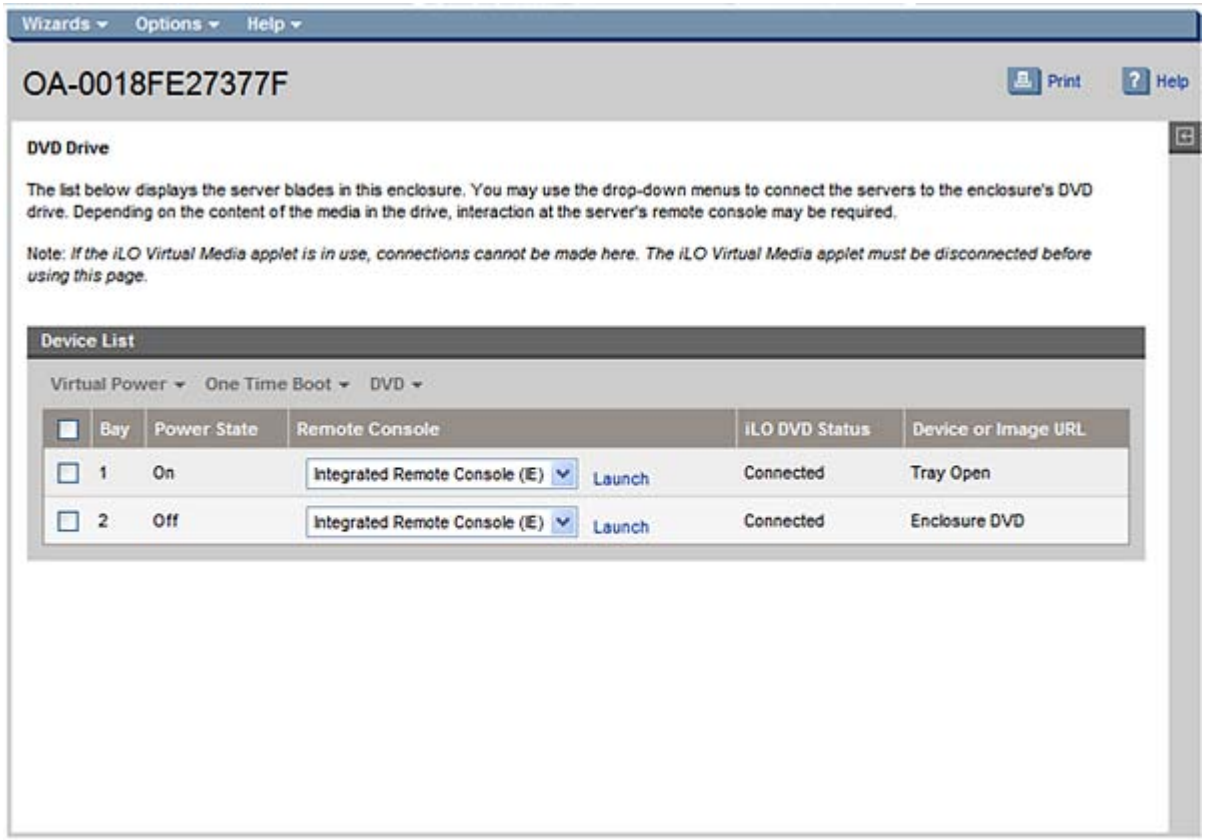
Si besoin, éjectez le disque du lecteur de DVD et insérez le disque d'installation suivant. Si le lecteur de DVD n'est pas occupé (pendant au moins 16 secondes), cliquez sur le bouton **DVD Drive Tray Open** (Plateau de lecteur de DVD ouvert). Le lecteur de DVD du boîtier n'est pas accessible ni contrôlable à partir de la fenêtre Virtual Media de la console distante intégrée.

Vous pouvez éjecter le support du lecteur de DVD via l'option de menu Éjecter du système d'exploitation sur la lame connectée au lecteur.



Une fois le support éjecté du lecteur de DVD/CD-ROM, le système d'exploitation vous invite à insérer un DVD ou CD.

À la suite de l'émission d'une commande d'éjection par le système d'exploitation, le périphérique de lame ou l'URL de l'image affiche `Tray Open` (Plateau ouvert). Toutefois, l'unité physique ne s'ouvre pas tant que vous n'appuyez pas sur le bouton d'ouverture du plateau à l'avant du lecteur de DVD.


Wizards
Options
Help
OA-0018FE27377F
Print
Help
DVD Drive
The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.
Note: If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.
Device List
Virtual Power
One Time Boot
DVD
Bay
Power State
Remote Console
iLO DVD Status
Device or Image URL
1
On
Integrated Remote Console (E)
Launch
Connected
Tray Open
2
Off
Integrated Remote Console (E)
Launch
Connected
Enclosure DVD

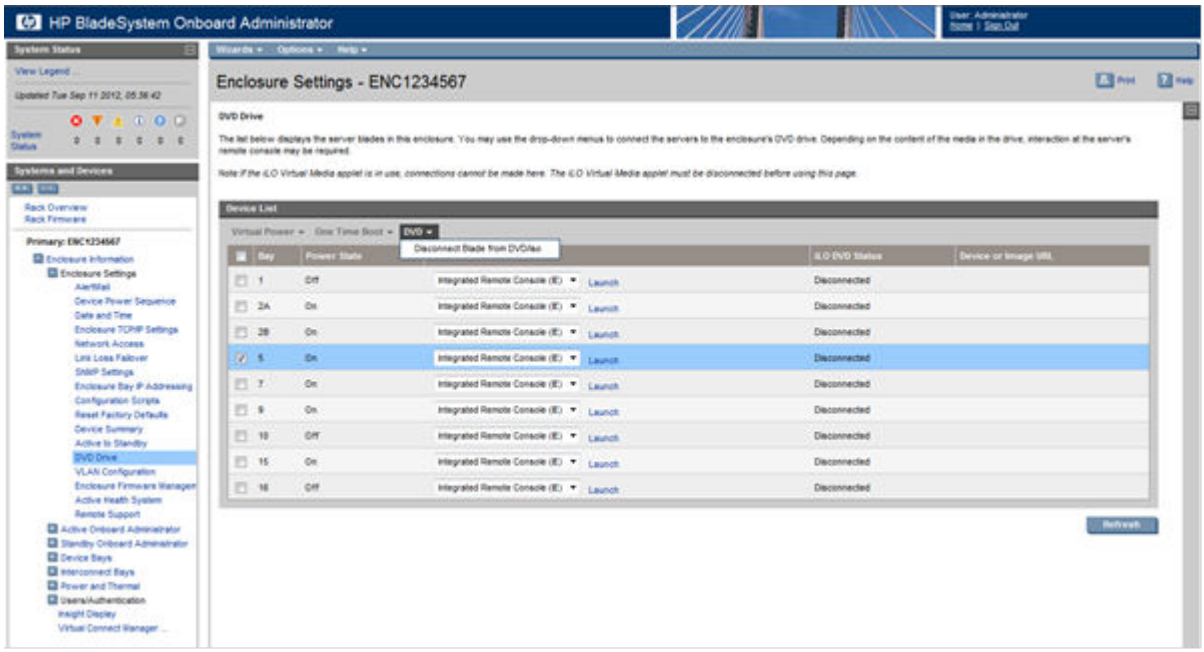
Vous pouvez insérer et éjecter des supports selon les besoins en fonction des directives de votre système d'exploitation, votre applications et vos données.

Déploiement sans assistance de système d'exploitation

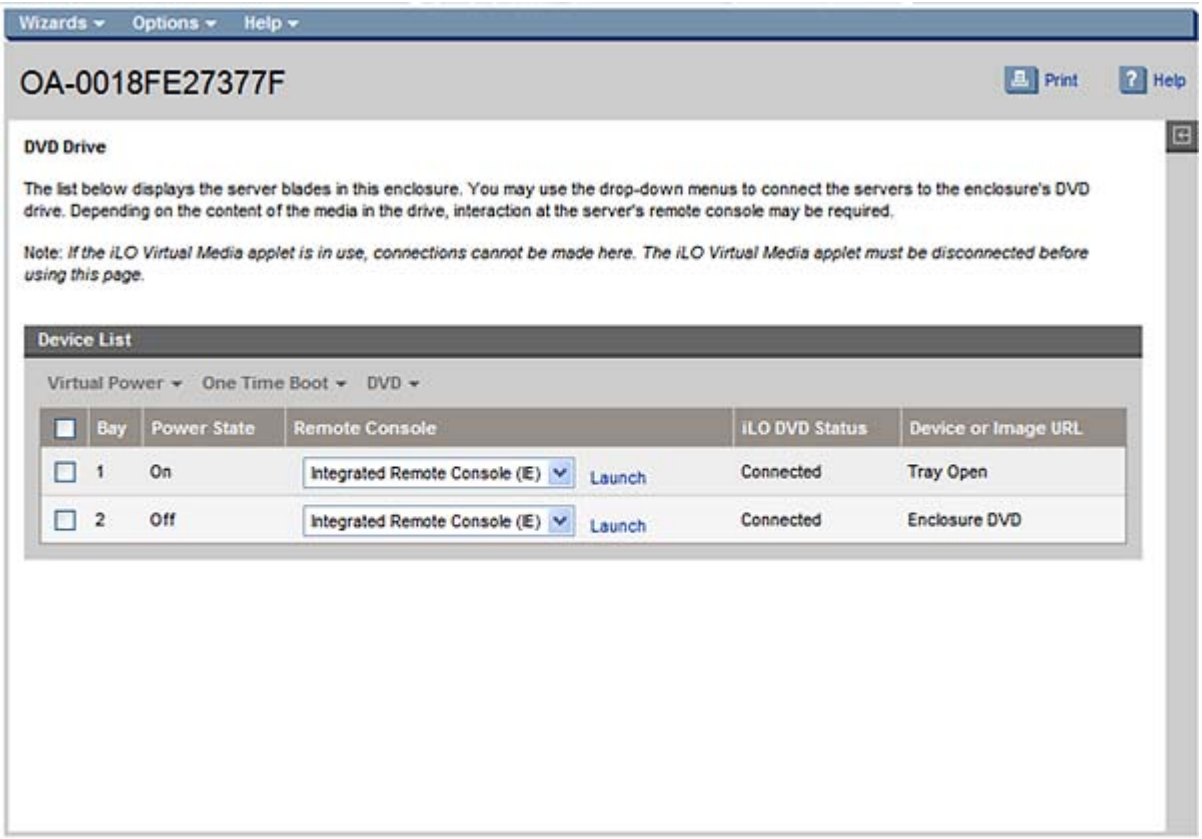
Le module Onboard Administrator peut approvisionner en silence de une à huit lames en utilisant le lecteur de DVD/CD-ROM partagé. Le disque de « build » utilisé dans le lecteur de DVD/CD-ROM doit pouvoir démarrer la lame, détecter le matériel de lame, créer des partitions de disque local, ainsi que déployer un système d'exploitation sur la lame. Ce type de mise en œuvre ne requiert qu'un seul disque et ne nécessite pas d'éjection de support. Les applications suivantes peuvent également être installées de la même manière, à condition que l'application tienne sur un disque unique.

Pour accéder au support dans un lecteur de DVD de lame :

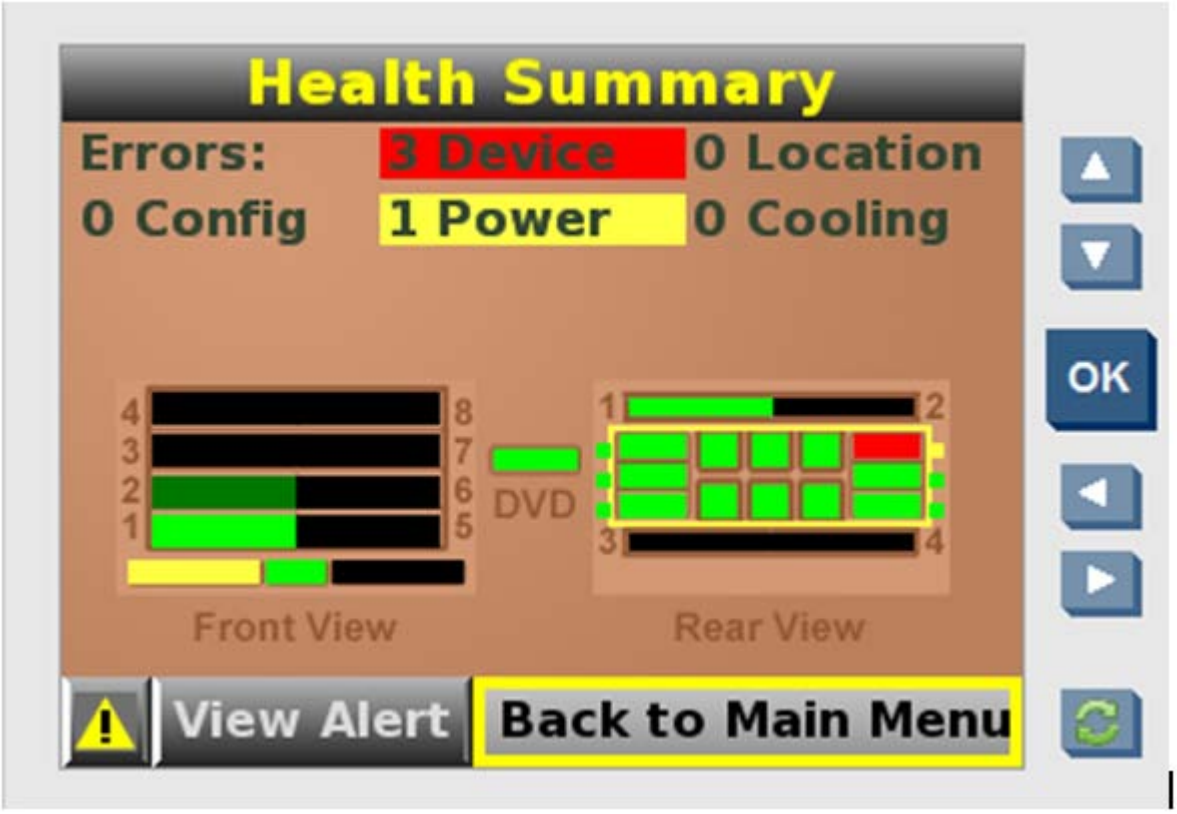
1. Connectez la lame à l'unité en naviguant vers la page du lecteur de DVD/CD-ROM.
2. Accédez à la page de mappage de la liste de périphériques.
3. Sélectionnez le menu DVD, puis sélectionnez **Connect to Enclosure DVD** (Connecter au DVD du boîtier).
4. Insérez le support dans le lecteur de DVD/CD-ROM avant d'effectuer la connexion.



Une fois le support inséré dans le lecteur de DVD, vous pouvez mettre sous tension ou redémarrer la lame via les options de menu correspondantes du lecteur de DVD sur la page de mappage de la liste de périphériques.


Wizards
Options
Help
OA-0018FE27377F
Print
Help
DVD Drive
The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.
Note: If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.
Device List
Virtual Power
One Time Boot
DVD
Bay
Power State
Remote Console
iLO DVD Status
Device or Image URL
1
On
Integrated Remote Console (IE)
Launch
Connected
Tray Open
2
Off
Integrated Remote Console (IE)
Launch
Connected
Enclosure DVD

Vous pouvez démarrer un déploiement sans assistance de système d'exploitation sur l'écran Insight Display. Pour débuter le processus d'installation, connectez le lecteur de DVD/CD-ROM, puis redémarrez le serveur. Insérez le DVD ou CD dans le lecteur de DVD/CD-ROM. L'écran Health Summary de l'écran Insight Display présente un état vert, indiquant qu'un support est inséré dans l'unité. Vous pouvez uniquement connecter des lames au lecteur de DVD une fois le support inséré. Les performances peuvent varier lorsque le nombre de lames augmente.

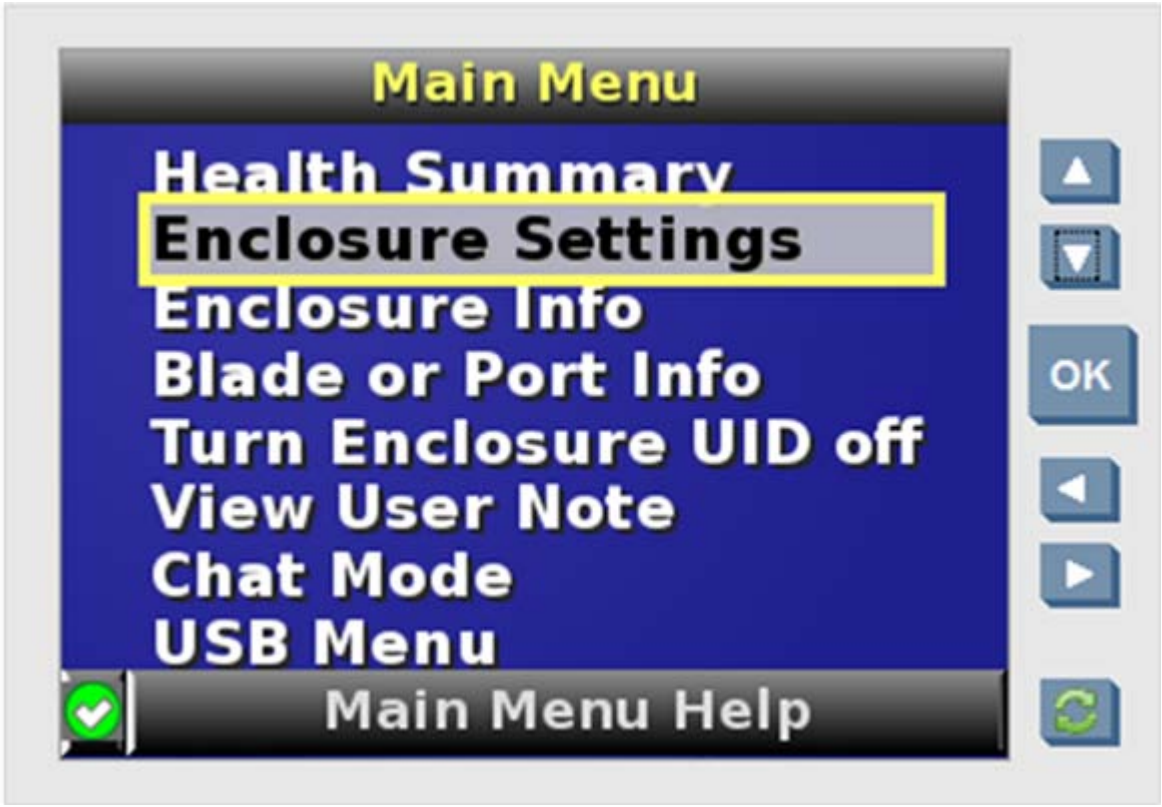


L'écran Insight Display présente l'état du lecteur de DVD/CD-ROM sur l'écran Health Summary sous forme d'icône de DVD avec une des couleurs suivantes :

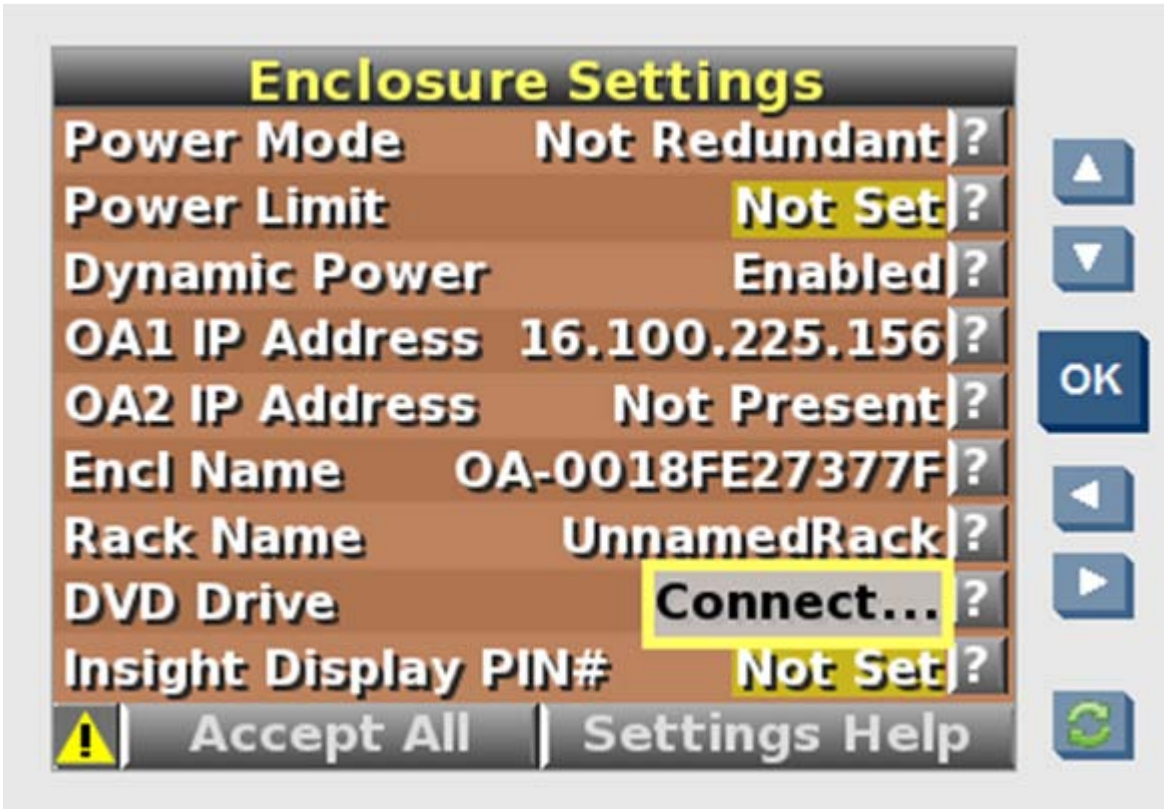
- Noir : aucune unité présente
- Gris clair : unité présente, mais aucun support présent
- Vert foncé : support présent déconnecté
- Vert clair : support présent connecté

Le menu principal de l'écran Insight Display permet de connecter des lames au lecteur de DVD/CD-ROM, puis de redémarrer les lames.

Dans le menu principal, sélectionnez **Enclosure Settings** (Paramètres du boîtier).



Dans l'écran Enclosure Settings du lecteur de DVD, sélectionnez **Connect** (Connexion).



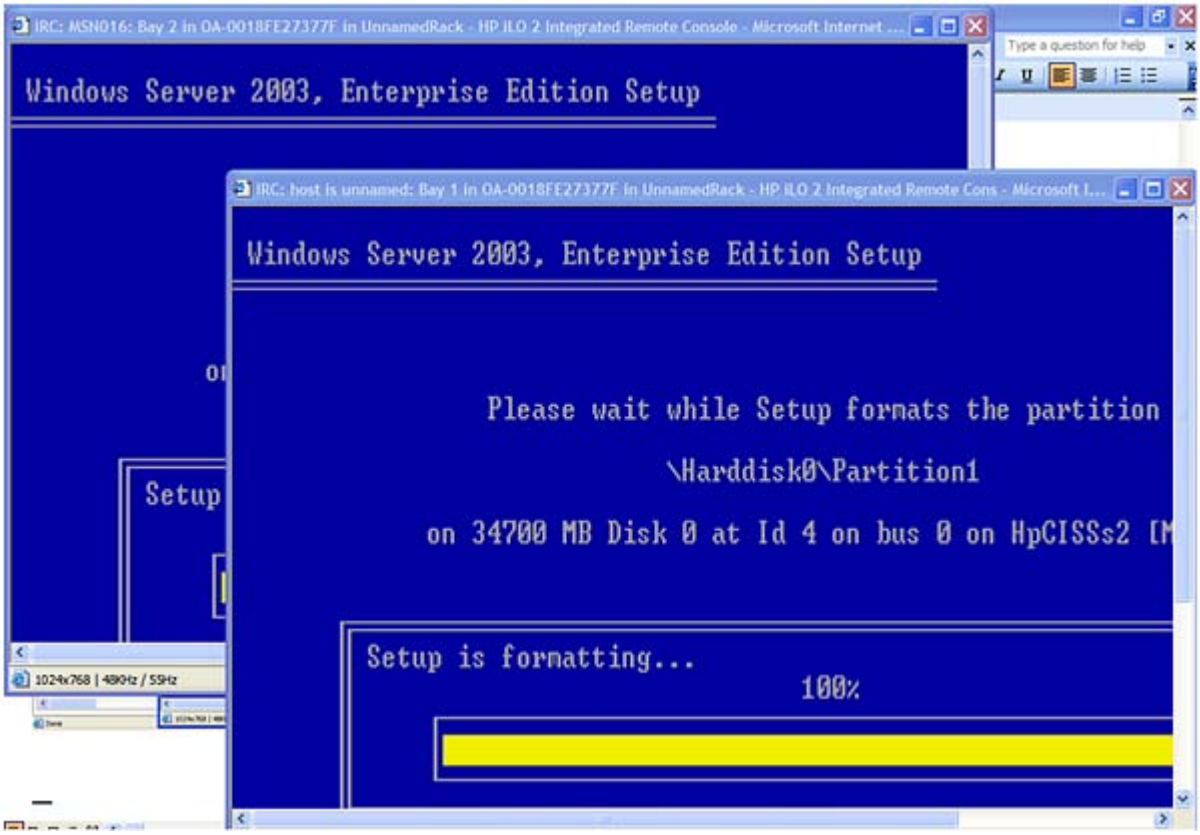
Dans l'écran DVD Connection Status (État de connexion de DVD), sélectionnez **All Blades** (Toutes les lames).

Sélectionnez **Connect to Enclosure DVD** (Connexion à l'unité de DVD du boîtier) dans l'écran Blade DVD Connection (Connexion de l'unité de DVD de lame).

Dans l'écran Connect : Blade DVD (Connecter : DVD de lame), sélectionnez **Connect and Reboot** (Connecter et redémarrer).

Toutes les lames redémarrent avec le lecteur de DVD/CD-ROM connecté. Si le support dans le lecteur de DVD/CD-ROM est amorçable, les lames démarrent à partir de ce support. Si une partition existe, le serveur peut essayer de démarrer à partir du disque dur local. Si les lames sont plus anciennes ou ont été effacées, supprimez et recréez les partitions d'unité locale.

Pour afficher l'avancement de l'installation sans assistance, utilisez la console distante intégrée.


Windows Server 2003, Enterprise Edition Setup
Windows Server 2003, Enterprise Edition Setup
Please wait while Setup formats the partition
\Harddisk0\Partition1
on 34700 MB Disk 0 at Id 4 on bus 0 on HpCISSs2
Setup is formatting...
100%
Setup

Accès ad-hoc au support basé sur DVD pour installation d'application ou importation de données

Utilisez le lecteur de DVD/CD-ROM basé sur boîtier pour insérer des CD ou DVD pour réaliser des tâches telles que l'installation d'une application ou le chargement de données à partir d'un CD. Ces tâches peuvent être effectuées suivant les besoins. Sa fonction principale est lorsque le lecteur de DVD n'est pas utilisé comme périphérique de démarrage.

Mise à jour de microprogramme de lame avec HP Smart Update Manager

Utilisez le lecteur de DVD du boîtier HP BladeSystem et le support de maintenance du microprogramme pour mettre à jour les ROM sur toutes les lames de serveur. Créez le DVD de maintenance du microprogramme pour construire un DVD amorçable. Insérez le DVD dans le lecteur de DVD partagé, connectez toutes les lames de serveur au lecteur, puis redémarrez le système. Le DVD de maintenance du microprogramme s'exécute sur toutes les lames de serveur connectées à l'unité de DVD.

Pour plus d'informations sur l'utilitaire HP Smart Update Manager, consultez le *Manuel de l'utilisateur de HP Smart Update Manager*. Pour plus d'informations sur la mise à jour du microprogramme sur des lames de serveur, reportez-vous au document *HP BladeSystem ProLiant Firmware Management Best Practices*.

Configuration VLAN

Le module Onboard Administrator version 3.00 ou ultérieure fournit un réseau VLAN marqué IEEE 802.1Q et configurable par l'utilisateur. Cette fonction permet d'isoler complètement le trafic à partir du serveur ou du module d'interconnexion en créant un réseau VLAN sur le réseau de supervision du boîtier.

Le réseau VLAN n'impose aucune exigence ou restriction sur l'adresse IP. Toutefois, le routeur ou commutateur externe, auquel le module Onboard Administrator est connecté, doit être configuré en tant que mode VLAN trunk pour acheminer et transmettre des trames Ethernet avec balises VLAN pour plusieurs VLAN passant par l'interface Ethernet externe du module Onboard Administrator.

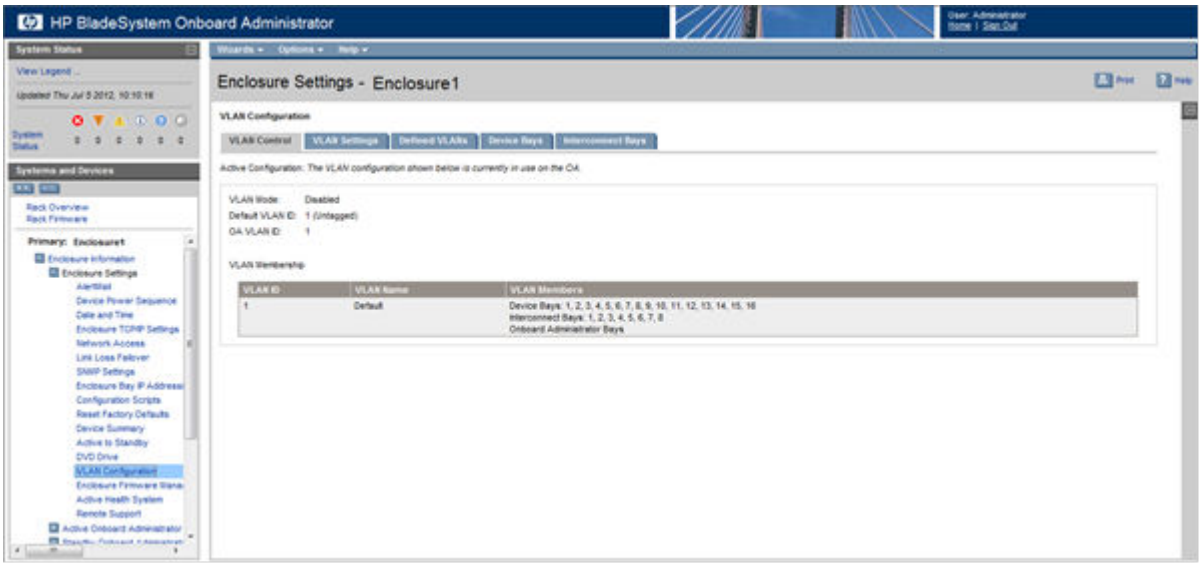
Caractéristiques VLAN

- L'ID VLAN est un numéro unique qui identifie chaque réseau VLAN. La plage autorisée des numéros d'ID VLAN est comprise entre 1 et 4094. Par défaut, le réseau VLAN est désactivé et tous les périphériques sont définis à ID VLAN 1. Après avoir configuré un réseau VLAN, les périphériques ne possédant pas le même ID VLAN ne peuvent pas communiquer entre eux.
- Toutes les trames non marquées reçues par le module Onboard Administrator sont affectées à l'ID VLAN par défaut. Le module Onboard Administrator répond avec des trames non marquées. Toutes les trames marquées ont un ID VLAN ou une balise dans la trame et le module Onboard Administrator répond avec des trames marquées.
- Si une trame marquée est envoyée à l'aide de l'ID VLAN par défaut, elle est ignorée par le module Onboard Administrator car ce dernier s'attend à ce que les trames d'ID VLAN par défaut ne soient pas marquées. Si la destination est pour le serveur ou une interconnexion, le module Onboard Administrator répond avec des trames non marquées.
- Le trafic entre le module iLO/IOM et le commutateur Broadcom n'est pas marqué, ce qui fait que le réseau VLAN est transparent. Le trafic entrant destiné au périphérique est marqué par le module Onboard Administrator allant vers le commutateur Broadcom qui supprime ensuite la marque avant d'envoyer le trafic au périphérique. Le commutateur Broadcom ajoute l'ID VLAN par défaut au port auquel le périphérique est relié, vers le trafic sortant du périphérique avant de l'envoyer.
- L'ID VLAN du serveur, du module d'interconnexion et du module Onboard Administrator peut être configuré de manière à autoriser le module Onboard Administrator à faire partie de n'importe quel réseau en configurant l'ID VLAN de telle sorte qu'elle corresponde au paramètre VLAN par défaut du commutateur externe auquel le module Onboard Administrator est connecté.
- Le microprogramme Onboard Administrator affecte l'ID VLAN par défaut à toutes les baies non configurées. L'ID VLAN par défaut peut être modifié par l'utilisateur. Vous pouvez associer un nom, limité à 31 caractères alphanumériques, à un ID VLAN. Vous pouvez enregistrer jusqu'à 25 entrées VLAN avec un ID VLAN et un nom à la fois.
- Le réseau VLAN prend en charge la communication pair-pair d'interconnexion SAS. Il existe également une prise en charge intégrale de l'interface de ligne de commande et de l'interface graphique, ainsi qu'une prise en charge limitée de l'affichage LCD. Vous pouvez activer et désactiver le réseau VLAN et afficher ou modifier les ID VLAN au travers du module Insight Display. Il n'existe pas de prise en charge VLAN sur la liaison et le port de service du boîtier.
- Les modules Onboard Administrator actif et en mode Standby sont définis sur les mêmes paramètres de configuration VLAN, ce qui fait que toutes les modifications apportées au module Onboard Administrator actif sont également effectuées sur le module Onboard Administrator en mode Standby. Aucune modification ne peut être apportée au module Onboard Administrator en mode Standby, mais vous pouvez visualiser les paramètres.
- Vous pouvez configurer ou modifier les paramètres VLAN avec un réseau VLAN désactivé. Les modifications effectuées par l'utilisateur lors de l'exécution sont enregistrées uniquement dans la mémoire RAM et sont perdues au redémarrage du module Onboard Administrator. Utilisez la commande `Save Config` pour enregistrer les modifications de configuration de manière permanente.

- Vous pouvez configurer le réseau VLAN à distance. Les modifications de configuration VLAN sont enregistrées uniquement dans la mémoire RAM, et elles sont ignorées au redémarrage sauf si vous les enregistrez dans une mémoire FLASH.
- Les périphériques sur différents réseaux de domaine VLAN ne peuvent pas communiquer. L'ensemble des serveurs et modules d'interconnexion, quel que soit leur ID VLAN, peuvent toujours être supervisés à l'aide du module Onboard Administrator. La machine client et le module Onboard Administrator doivent être sur le même ID VLAN pour accéder au module Onboard Administrator.

HP recommande d'utiliser un terminal de console pour configurer votre réseau afin d'éviter toute perte de communication lors de la modification de la configuration VLAN. Les modifications correspondantes doivent ensuite être effectuées sur le commutateur externe auquel ce module Onboard Administrator est connecté.

L'onglet VLAN Control (Contrôle VLAN) affiche la configuration active actuellement utilisée sur le module Onboard Administrator.



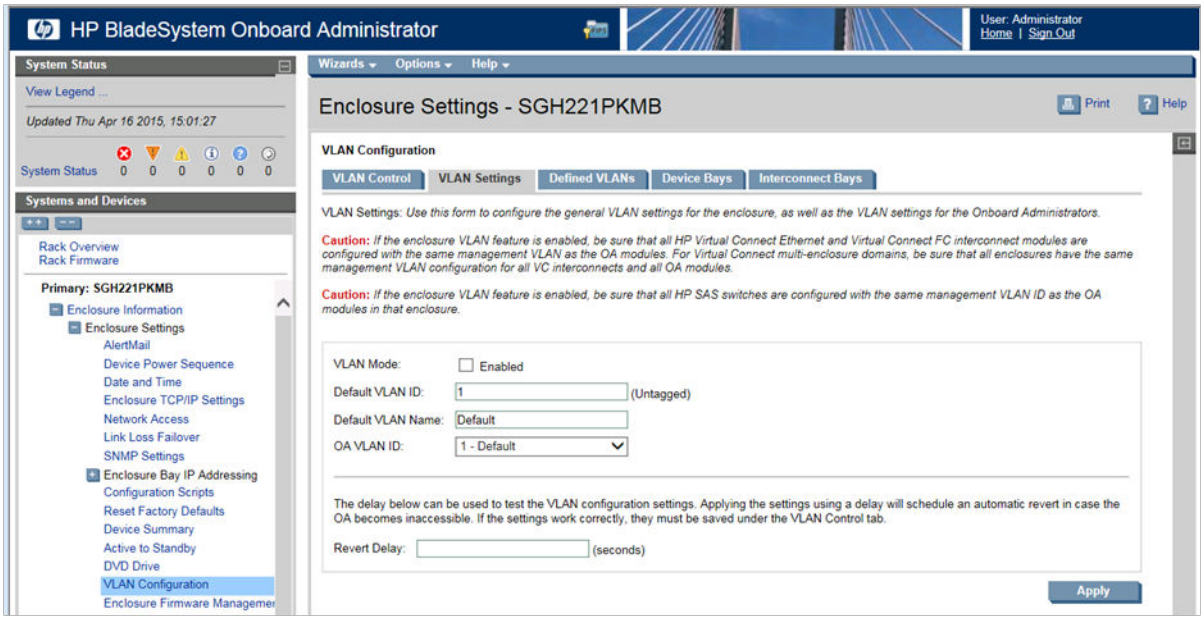
Paramètres VLAN

Les paramètres VLAN généraux et les paramètres VLAN du module Onboard Administrator sont configurés à partir de l'onglet VLAN Settings (Paramètres VLAN). Les paramètres des baies de périphériques et d'interconnexion sont configurés à partir des onglets Device Bays et Interconnect Bays. Une fois des modifications apportées à l'un de ces trois onglets, l'onglet VLAN Control (Contrôle VLAN) s'affiche. Une fois l'onglet VLAN Control (Contrôle VLAN) affiché, vous pouvez enregistrer les paramètres ou revenir aux paramètres précédents.

Le délai de régression sur l'onglet des paramètres VLAN est utilisé pour planifier une régression des paramètres sur ce qui est actuellement enregistré sur le module Onboard Administrator. Ceci peut être utilisé si vous administrez les paramètres à distance et devenez déconnecté. Si vous configurez de manière incorrecte les paramètres VLAN et devenez déconnecté, les paramètres VLAN du module Onboard Administrator reviennent à leur état antérieur avant la déconnexion.

⚠ **ATTENTION :** Si la fonction VLAN du boîtier est activée, assurez-vous que tous les modules d'interconnexion HP Virtual Connect Ethernet et Virtual Connect FC sont configurés avec le même réseau VLAN de supervision que les modules OA. Pour les domaines multi-boîtiers Virtual Connect, assurez-vous que tous les boîtiers ont la même configuration VLAN de supervision pour tous les modules d'interconnexion VC et tous les modules OA.

⚠ **ATTENTION :** Si la fonction VLAN du boîtier est activée, assurez-vous que tous les commutateurs HP SAS sont configurés avec le même ID VLAN de supervision que les modules OA dans ce boîtier.


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
System Status
View Legend ...
Updated Thu Apr 16 2015, 15:01:27
System Status 0 0 0 0 0 0
Systems and Devices
Rack Overview
Rack Firmware
Primary: SGH221PKMB
Enclosure Information
Enclosure Settings
AlertMail
Device Power Sequence
Date and Time
Enclosure TCP/IP Settings
Network Access
Link Loss Failover
SNMP Settings
Enclosure Bay IP Addressing
Configuration Scripts
Reset Factory Defaults
Device Summary
Active to Standby
DVD Drive
VLAN Configuration
Enclosure Firmware Manageme
Wizards
Options
Help
Enclosure Settings - SGH221PKMB
Print
Help
VLAN Configuration
VLAN Control
VLAN Settings
Defined VLANs
Device Bays
Interconnect Bays
VLAN Settings: Use this form to configure the general VLAN settings for the enclosure, as well as the VLAN settings for the Onboard Administrators.
Caution: If the enclosure VLAN feature is enabled, be sure that all HP Virtual Connect Ethernet and Virtual Connect FC interconnect modules are configured with the same management VLAN as the OA modules. For Virtual Connect multi-enclosure domains, be sure that all enclosures have the same management VLAN configuration for all VC interconnects and all OA modules.
Caution: If the enclosure VLAN feature is enabled, be sure that all HP SAS switches are configured with the same management VLAN ID as the OA modules in that enclosure.
VLAN Mode:
Enabled
Default VLAN ID:
1
(Untagged)
Default VLAN Name:
Default
OA VLAN ID:
1 - Default
The delay below can be used to test the VLAN configuration settings. Applying the settings using a delay will schedule an automatic revert in case the OA becomes inaccessible. If the settings work correctly, they must be saved under the VLAN Control tab.
Revert Delay:
(seconds)
Apply

Mode VLAN (Mode VLAN) : le paramètre par défaut du mode VLAN est désactivé. Pour activer les paramètres VLAN, cochez cette case.

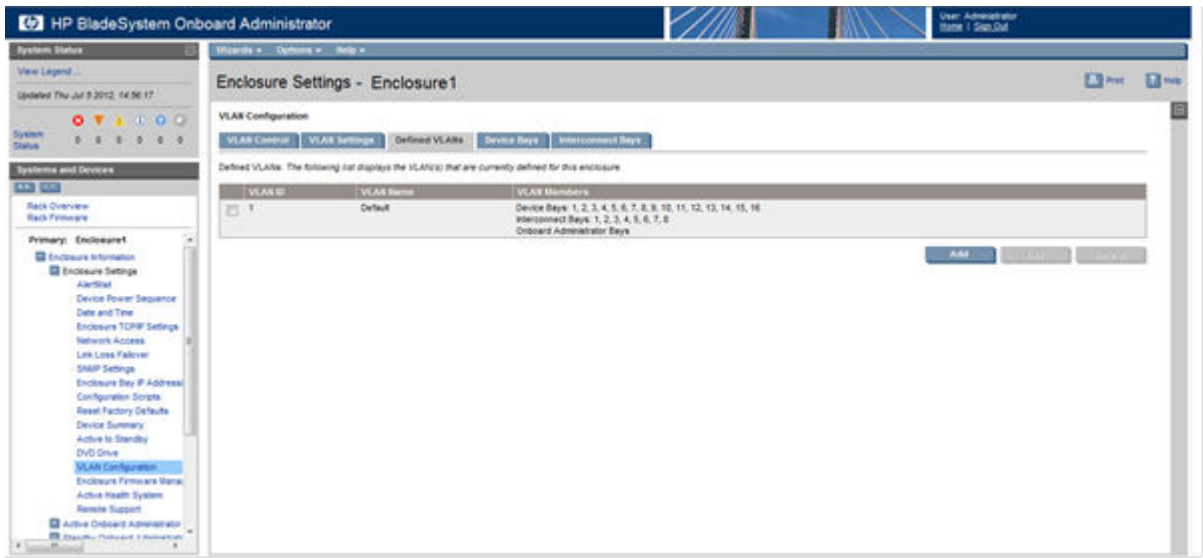
Paramètre	Description
Default VLAN ID	Numéro d'ID VLAN par défaut actuel. Les valeurs possibles de l'ID VLAN sont 1 à 4094.
Default VLAN Name	Nom d'ID VLAN par défaut actuel. Ce champ est facultatif et limité à 31 caractères au maximum, y compris caractères alphanumériques, tirets (-), caractères de soulignement (_) et espaces.
OA VLAN ID	ID VLAN du module OA actuel. Pour modifier l'appartenance du module Onboard Administrator, sélectionnez un VLAN défini à partir du menu. La modification d'appartenance s'appliquera au module Onboard Administrator actif et au module Onboard Administrator en mode Standby.
Revert Delay (Délai de régression)	Ce paramètre vous permet de revenir automatiquement à la configuration VLAN actuellement enregistrée si vous êtes déconnecté après avoir apporté des modifications de configuration VLAN.

Pour enregistrer temporairement des modifications apportées à la configuration VLAN, cliquez sur **Apply** (Appliquer).

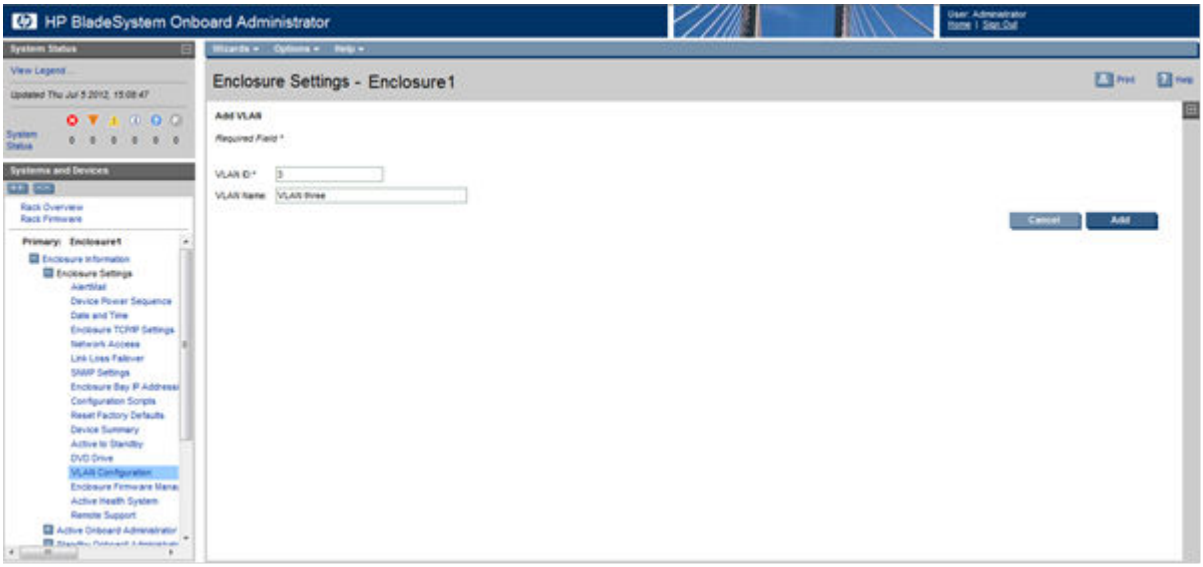
L'onglet VLAN Control (Contrôle VLAN) s'affiche afin que vous puissiez enregistrer de manière permanente les modifications de configuration ou revenir à la configuration précédemment enregistrée.

Ajout, édition et suppression de réseaux VLAN

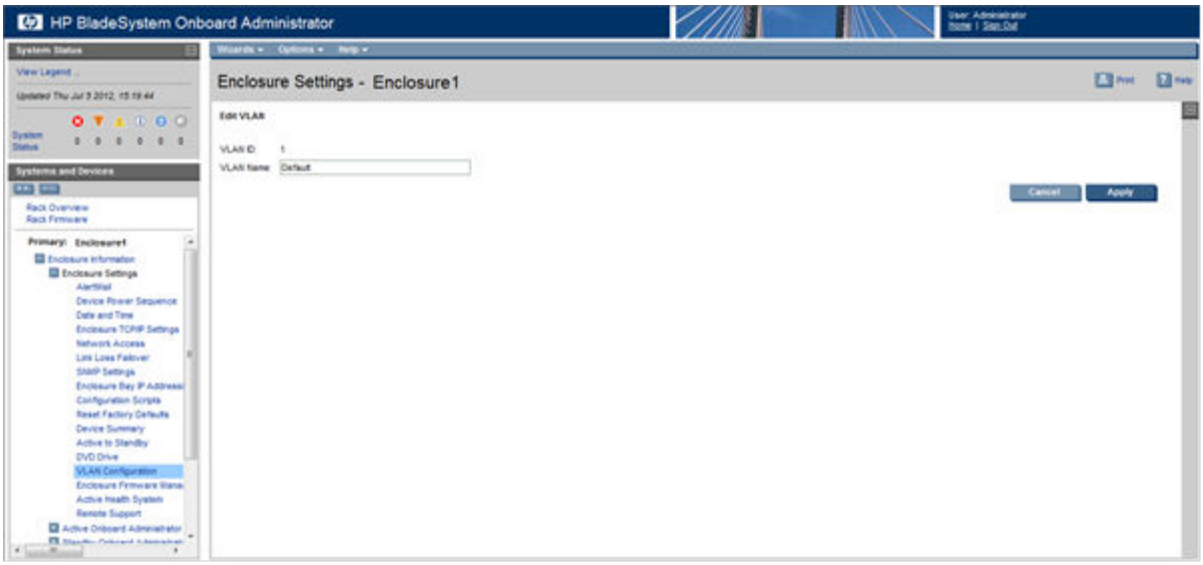
Pour ajouter un nouveau réseau VLAN, cliquez sur l'onglet **Defined VLANs** (VLAN définis), puis cliquez sur **Add** (Ajouter).



La page Add VLAN (Ajouter un réseau VLAN) s'affiche avec deux champs : VLAN ID (ID VLAN) et VLAN Name (Nom VLAN). Le champ VLAN Name est facultatif. L'ID VLAN doit être un entier compris entre 1 et 4094. Si vous tentez d'ajouter un nouveau réseau VLAN où le nom et l'ID correspondent à un réseau VLAN existant, un message d'erreur apparaît.



Le nom d'un réseau VLAN existant peut être modifié en naviguant vers l'onglet **Defined VLANs** (VLAN définis). Sélectionnez un réseau VLAN, puis cliquez sur **Edit** (Modifier). La page Edit VLAN (Modifier réseau VLAN) apparaît avec un champ qui permet de modifier le nom du réseau VLAN. Le nom VLAN n'est pas un champ obligatoire.



Les réseaux VLAN existants peuvent être supprimés de la page Defined VLANs (VLAN définis) en sélectionnant des réseaux VLAN, puis en cliquant sur **Delete** (Supprimer). La suppression d'un réseau VLAN supprime tous ses membres dans le réseau VLAN par défaut. Le réseau VLAN par défaut ne peut pas être supprimé.

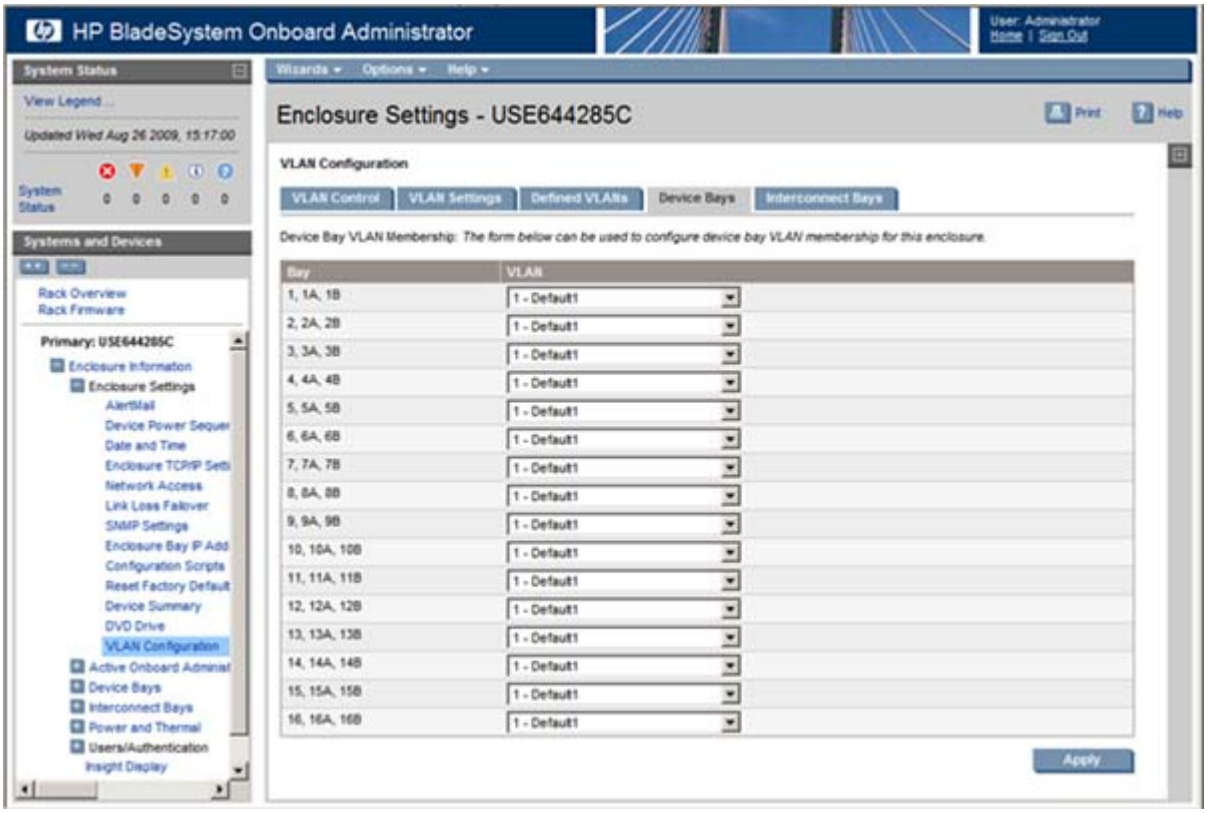
REMARQUE : L'accès au module OA actif via l'adresse IPv6 d'un lien-local est susceptible de ne pas fonctionner sur certaines configurations système client contenant plusieurs interfaces réseau.

Configuration de périphériques

Une fois des réseaux VLAN définis via l'onglet Defined VLANs (VLAN définis), des périphériques peuvent être affectés pour les utiliser. Le module Onboard Administrator est affecté à un réseau VLAN sous l'onglet VLAN Settings (Paramètres VLAN). Les baies de périphériques et les baies d'interconnexion sont affectées sous les onglets Device Bays et Interconnect Bays.

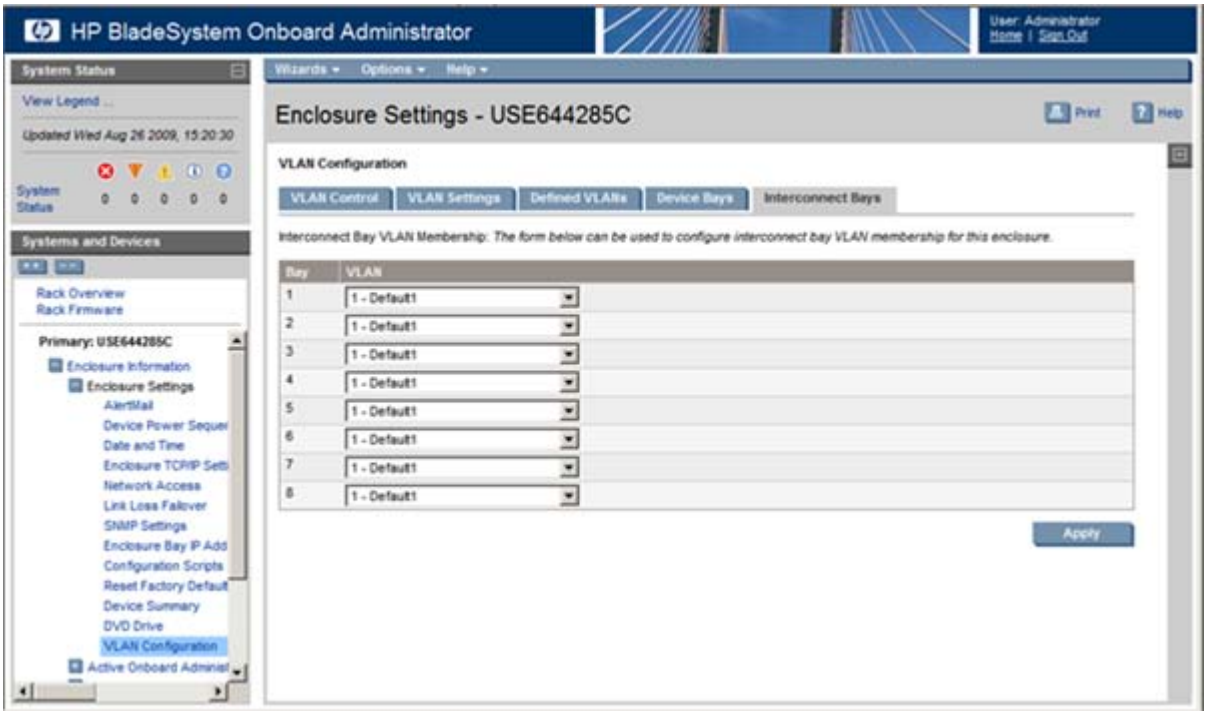
Baies de périphérique

Pour modifier l'appartenance d'une baie de périphérique, sélectionnez un réseau VLAN défini dans le menu situé sous la colonne VLAN, puis cliquez sur **Apply** (Appliquer).

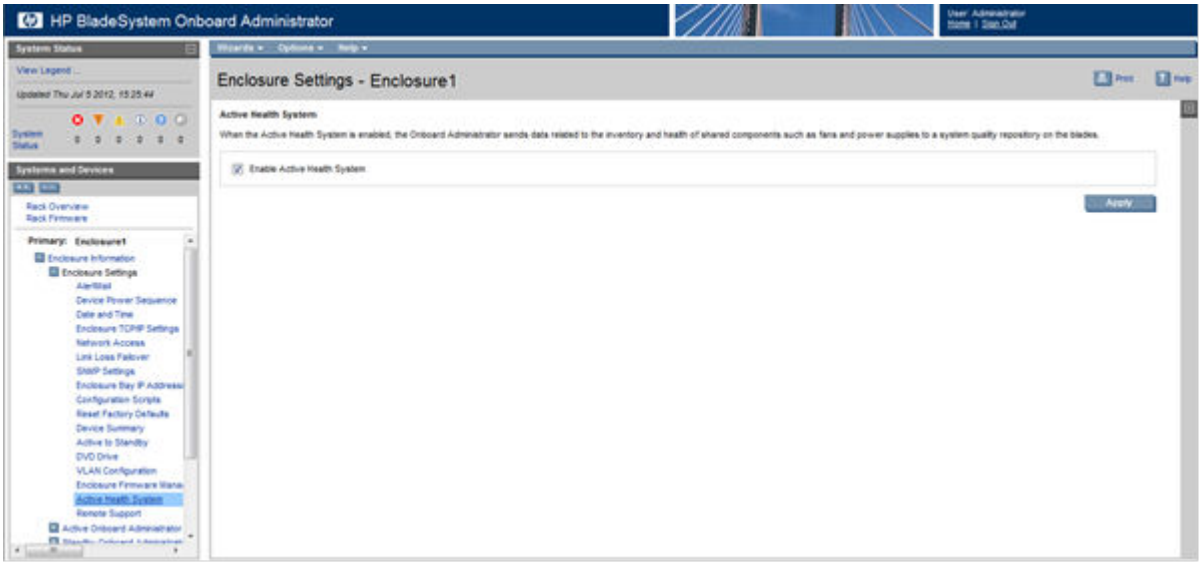


Baies d'interconnexion

Pour modifier l'appartenance d'une baie d'interconnexion, sélectionnez un réseau VLAN défini dans le menu situé sous la colonne VLAN, puis cliquez sur **Apply** (Appliquer).



Active Health System



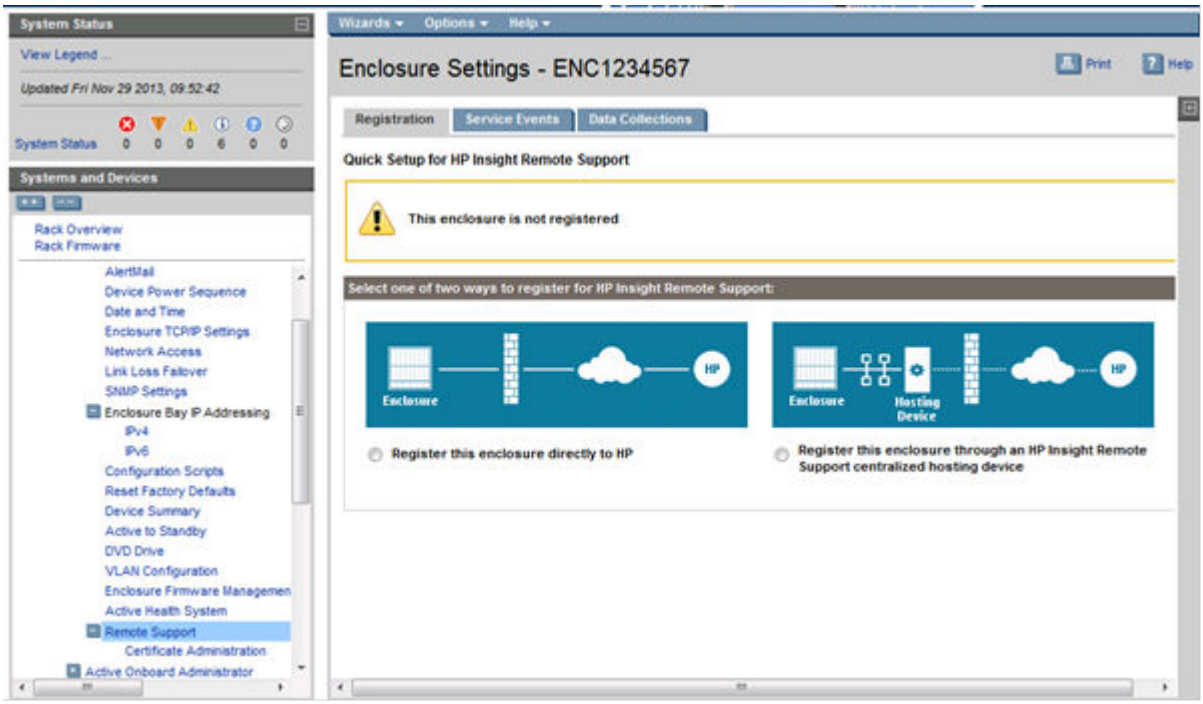
HP Active Health System surveille et enregistre les modifications apportées au matériel du serveur et à la configuration du système. Active Health System permet de diagnostiquer les problèmes et d'aboutir à une résolution rapide en cas de pannes du serveur. Dans un boîtier HP BladeSystem, le module Onboard Administrator fournit des données relatives aux paramètres système et aux composants partagés de l'infrastructure au module Active Health System situé sur les lames de serveur HP ProLiant. L'outil HP Active Health System ne recueille pas de données sur les opérations, finances, clients, employés, partenaires ou centres de données de l'utilisateur de HP Active Health System (par exemple, adresses IP, noms d'hôte, noms d'utilisateur et mots de passe). Des exemples de données recueillies par le module Onboard Administrator incluent des informations d'état et d'inventaire pour les paramètres et composants suivants :

- Ventilateurs de boîtier
- Alimentations de boîtier
- Modules d'interconnexion
- Fond de panier central de boîtier
- Onboard Administrators

Mesures d'alimentation de boîtier

Inscription à Insight Remote Support

L'écran suivant affiche l'onglet Remote Support Registration, avec le boîtier qui n'est pas encore inscrit :



L'écran suivant affiche l'onglet Remote Support Registration, avec le boîtier inscrit :

HP a développé un service et une expérience de prise en charge qui automatisent de nombreuses tâches quotidiennes et vous aident à réduire les risques. HP intègre un tableau de bord personnalisé en ligne (HP Insight Online), un portail et une application mobile de prise en charge (HP Support Center Mobile), et une prise en charge à distance 24h/24 et 7j/7 (HP Insight Remote Support) pour l'infrastructure consolidée.

Lorsque vous utilisez la fonctionnalité Remote Support intégrée avec un boîtier HP BladeSystem c-Class, vous pouvez choisir parmi les options suivantes de configuration :

- **Insight Online direct connect** : inscrivez un boîtier pour communiquer directement avec HP Insight Online sans configurer de périphérique d'hébergement centralisé HP Insight Remote Support dans votre environnement local. HP Insight Online sera votre principale interface pour

les informations d'assistance à distance. La configuration de connexion directe est disponible dans Onboard Administrator 4.11 et versions ultérieures.

- **Insight Remote Support central connect** : inscrivez un boîtier pour communiquer avec HP via un périphérique d'hébergement centralisé HP Insight Remote Support dans votre environnement local. Toutes les informations d'événements de configuration et de service sont acheminées à travers le périphérique d'hébergement. Ces informations peuvent être consultées à l'aide de la console HP Insight RS locale ou de la vue Web dans HP Insight Online. La configuration de connexion centrale est disponible sur Onboard Administrator 3.60 et versions ultérieures.

Données collectées par Insight Remote Support

Lorsque le boîtier BladeSystem est inscrit auprès de Insight Remote Support, les informations suivantes concernant les composants de l'infrastructure partagée du boîtier BladeSystem dans le boîtier sont envoyées à HP :

- Inscription : dans le cadre de la procédure d'inscription du boîtier, pour une connexion centrale, le module Onboard Administrator envoie au périphérique d'hébergement Insight Remote Support les données qui identifient de manière unique le matériel du boîtier. Pour une connexion directe, le module Onboard Administrator envoie les données directement à un service Web dans le centre de données Remote Support.

  Des exemples de données collectées incluent les suivants :

  - Nom du boîtier
  - Nom de produit du boîtier
  - Référence du boîtier
  - Numéro de série du boîtier
  - Nom du fabricant du boîtier
  - Version du microprogramme Onboard Administrator
  - Adresses IP et MAC du module Onboard Administrator

- Événements de service : dans le cadre du processus des événements de service, le module Onboard Administrator envoie des données pour identifier de manière unique le composant matériel pertinent au périphérique d'hébergement de Insight Remote Support.

  Des exemples de données collectées incluent les suivants :

  - Modèle du boîtier
  - Numéro de série du boîtier
  - Référence du composant matériel pertinent
  - Description, emplacement et autres caractéristiques d'identification du composant matériel pertinent

  Pour plus d'informations, consultez la section « Événements de service Insight Remote Support » (Événements de service Insight Remote Support à la page 190).

- Collectes de données : dans le cadre du processus de collecte de données, le module Onboard Administrator envoie des données au service Insight Remote Support pour activer des fonctions de conseils proactifs et de consulting. Les informations sont envoyées pour le matériel du boîtier ainsi que les composants système remplis, notamment le module LCD, les modules Onboard Administrator, les modules de ventilation de boîtier, les modules d'alimentation de boîtier, les modules d'interconnexion et les lames de serveur.

Des exemples de données collectées pour ces composants système incluent :

- Descripteurs de module matériel tels que fabricant, nom du produit, numéro de série, UUID, numéro de référence et emplacement dans le boîtier
- Révision du microprogramme
- Informations de diagnostic et d'état
- Informations d'état et de configuration d'alimentation et thermiques
- Informations de mappage de ports et réseau

Pour plus d'informations, consultez la section « Collectes de données Insight Remote Support » (Collectes de données Insight Remote Support à la page 192).

Conditions préalables requises

Avant d'entreprendre l'enregistrement, vérifiez que les conditions suivantes sont remplies :

- Une version prise en charge du microprogramme du module OA est installé sur tous les modules OA dans la boîtier.
  - La version 3.60 ou ultérieure est requise pour l'enregistrement pour Insight Remote Support central connect.
  - La version 4.11 ou ultérieure est requise pour l'enregistrement pour Insight Online direct connect.

  Vous pouvez télécharger la version du microprogramme la plus récente à partir du site Web HP (http://www.hp.com/go/oa).
- Pour Insight Online direct connect uniquement : un serveur DNS est configuré dans le module Onboard Administrator. Ceci est nécessaire pour les communications entre iLO et Insight Online.
- Pour Insight Remote Support central connect uniquement : Insight RS 7.0.5 ou version ultérieure est installé et configuré sur le périphérique d'hébergement Insight RS.

REMARQUE : Un certificat valide est requis en cas de connexion à un périphérique d'hébergement HP Insight Remote Support et si le module Onboard Administrator fonctionne en mode FIPS.

REMARQUE : Lorsque le module Onboard Administrator fonctionne en mode FIPS, la longueur minimale de la clé RSA ne doit pas être inférieure à 2 048 bits, et l'algorithme de hachage de la signature doit être SHA1, SHA-224, SHA-256, SHA-384 ou SHA-512.

Inscription à Insight Remote Support à l'aide de l'interface Web OA

HP Insight Remote Support permet l'envoi automatique des événements matériels à HP pour éviter les temps d'arrêt et permettre une résolution plus rapide du problème. Vous pouvez vous inscrire directement à HP ou à travers un périphérique d'hébergement de Insight RS.

Inscription à Insight Remote Support à l'aide de connexion directe

Pour enregistrer un boîtier HP BladeSystem c-Class pour Insight Online direct connect, utilisez la procédure suivante. Lorsque vous inscrivez un boîtier pour Insight Online direct connect, vous devez suivre les étapes de l'interface OA et du portail Insight Online.

1. Vérifiez que le système remplit les conditions requises pour l'utilisation de la solution Insight Remote Support. Pour plus d'informations, consultez la section « Conditions requises ».
2. Accédez à la page **Enclosure Information>Enclosure Settings>Remote Support**.

3. Dans l'onglet **Registration** (Inscription), sélectionnez **Register this enclosure directly to HP** (Inscrire ce boîtier directement auprès de HP). La page s'actualise pour afficher les options d'inscription pour une connexion directe.
4. Entrez vos informations d'identification HP Passport dans les champs **Nom d'utilisateur HP Passport** et **Mot de passe HP Passport**.

> **REMARQUE :** Entrez votre ID d'utilisateur HP Passport dans la section **Nom d'utilisateur HP Passport**. Dans la plupart des cas, votre ID d'utilisateur HP Passport est l'adresse électronique que vous avez utilisée au cours du processus d'inscription à HP Passport. Si vous avez modifié votre ID d'utilisateur dans HPSC, veillez à entrer votre ID d'utilisateur et non votre adresse électronique.

5. Facultatif : Si votre boîtier HP BladeSystem c-Class utilise un serveur proxy Web pour accéder à Internet, entrez les informations suivantes :
   - **Serveur proxy Web**
   - **Nom d'utilisateur de proxy Web**
   - **Mot de passe de proxy Web**
   - **Port de proxy Web**
6. Cochez la case **I accept the terms and conditions of the HP Software License Agreement and the HP Insight Management Additional License Authorization** (J'accepte les termes et conditions de l'Accord de licence logicielle HP et l'autorisation de licence supplémentaire HP Insight Management). Ces documents peuvent être consultés sur le site Web des documents de licences logicielles HP (http://www.hp.com/go/SWLicensing).
7. Cliquez sur **Register**. Le fait de cliquer sur **Register** est la première des deux étapes du processus d'inscription. L'étape 2 est effectuée dans HP Insight Online.

   En vous inscrivant, vous acceptez d'envoyer les données d'inscription, des événements de services et de configuration à HP. Toutes les données collectées et envoyées à HP sont gérées conformément à la déclaration de confidentialité des données HP. Vous pouvez afficher la déclaration de confidentialité des données HP sur le site Web de HP (http://www.hp.com/go/privacy).

   Lorsque l'étape 1 de la procédure d'inscription commence, le message suivant apparaît :

   ```
   Step 1 of registration in progress, please wait...
   ```

   Une fois l'étape 1 terminée, le message suivant s'affiche :

   ```
   Step 1 of remote support registration has been completed. Please
   proceed to step 2 to complete the registration process.
   ```

   Attendez 5 minutes pour que votre demande d'inscription soit entièrement traitée.
8. Accédez au site Web HP Insight Online (http://www.hp.com/go/insightonline.), puis connectez-vous avec vos identifiants de compte HP Passport.
9. Suivez les instructions à l'écran dans Insight Online, et indiquez les informations de site, contact et partenaire afin que HP puisse offrir un service pour votre boîtier. Pour obtenir des instructions détaillées, consultez le *Manuel d'installation de HP Insight Remote Support et Insight Online pour serveurs HP ProLiant et boîtiers HP BladeSystem c-Class*.
10. Revenez à la page **Remote Support** dans l'interface Web OA, cochez la case **Please confirm that you have completed the registration process in HP Insight Online** (Veuillez confirmer que vous avez effectué le processus d'inscription dans HP Insight Online), puis cliquez sur **Apply** (Appliquer).

Le message suivant apparaît :

```
Are you sure you have completed registration in HP Insight Online?
Click OK to confirm or Cancel to cancel.
```

11. Cliquez sur **OK**. Un message semblable à celui-ci s'affiche :

    ```
    Successfully registered!

    HP Passport User ID used to register this enclosure: <HP passport User
    ID>.
    ```

12. Facultatif : envoyez un événement de test pour confirmer la connexion entre OA et Insight Remote Support :
    a. Accédez à **Enclosure Settings > Remote Support.**
    b. Cliquez sur l'onglet **Service Events** (Événements de service Insight Remote Support à la page 190) (Événements de service Insight Remote Support à la page 190).
    c. Cliquez sur **Send Test Event** (Envoyer un événement de test).
13. Facultatif : Pour recevoir des alertes électroniques concernant des événements du système, configurez AlertMail sur la page **Enclosure Information>Enclosure Settings>AlertMail** (AlertMail à la page 117) (AlertMail à la page 117).

Modification des paramètres du proxy Web

Les paramètres de proxy doivent être conservés pour permettre à votre boîtier de continuer à envoyer des données Remote Support à HP. Si les paramètres de proxy changent, utilisez la procédure suivante pour les modifier :

1. Accédez à la page **Enclosure Information>Enclosure Settings>Remote Support**.
2. Le cas échéant, mettez à jour les paramètres suivants :
   - **Web Proxy Server** (Serveur de proxy Web) : entrez le serveur de proxy Web au format http://<nom_hôte ou adresse_IP>.
   - **Port de proxy Web**
   - **Nom d'utilisateur de proxy Web**
   - **Mot de passe de proxy Web**
3. Cliquez sur **Apply (Appliquer)**.

Inscription à Insight Remote Support à l'aide d'une connexion centrale

Pour enregistrer un boîtier HP BladeSystem c-Class pour Insight Remote Support central connect, utilisez la procédure suivante :

1. Vérifiez que le système remplit les conditions requises pour l'utilisation de Insight Remote Support. Pour plus d'informations, consultez la section « Conditions requises ».
2. Accédez à la page **Enclosure Information>Enclosure Settings>Network Access** (Accès réseau à la page 136) (Accès réseau à la page 136), puis cliquez sur l'onglet **Protocol**.
3. Vérifiez que la case Enable XML Reply (Activer réponse XML) sélectionnée.

   Si cette case n'est pas cochée, le périphérique d'hébergement Insight RS ne peut pas collecter de données à partir du module Onboard Administrator.
4. Accédez à la page **Enclosure Information>Enclosure Settings>Remote Support**.

5. Sélectionnez **Register this enclosure through an HP Insight Remote Support centralized hosting device** (Enregistrer ce boîtier par l'intermédiaire d'un périphérique d'hébergement centralisé HP Insight Remote Support). La page se met à jour pour afficher les options d'enregistrement de connexion centralisé.
6. Entrez le nom d'hôte du périphérique d'hébergement Insight RS ou l'adresse IP et le numéro de port. La valeur par défaut est 7906.
7. Cliquez sur **Register** (Enregistrer). En vous inscrivant, vous acceptez d'envoyer l'enregistrement, les événements de service et les données de configuration à HP. Toutes les données collectées et envoyées à HP sont gérées conformément à la déclaration de confidentialité des données HP. Vous pouvez afficher la déclaration de confidentialité des données HP sur le site Web de HP (http://www.hp.com/go/privacy). Le message suivant s'affiche :

   ```
   Device successfully registered.
   ```
8. Facultatif : envoyez un événement de test pour confirmer la connexion entre OA et Insight Remote Support :
   a. Accédez à **Enclosure Settings > Remote Support**.
   b. Cliquez sur l'onglet **Service Events** (Événements de service Insight Remote Support à la page 190) (Événements de service Insight Remote Support à la page 190).
   c. Cliquez sur **Send Test Event** (Envoyer un événement de test).

Désinscription d'un boîtier HP BladeSystem c-Class à partir de Insight Online direct connect

1. Accédez à la page **Enclosure Information>Enclosure Settings>Remote Support**.
2. cliquez sur **Désinscription** ;

   Le message suivant apparaît : `Are you sure you want to un-register and disable HP Insight Remote Support?.`
3. Cliquez sur **OK**.

   Le message suivant apparaît : `Un-registration in progress. Please wait...`

   Une fois l'annulation de l'inscription terminée, la page Remote Support affiche le message suivant :

   ```
   The enclosure is not registered.
   ```

Désinscription d'un boîtier HP BladeSystem c-Class à partir de Insight Remote Support central connect

1. Connectez-vous à la console Insight RS.
2. Effectuez l'une des actions suivantes :
   - Pour arrêter temporairement la surveillance d'un boîtier HP BladeSystem c-Class, sélectionnez le boîtier dans l'onglet **Devices>Device Summary** dans la console HP Insight RS, puis sélectionnez **ACTIONS>DISABLE SELECTED**.
   - Pour arrêter de façon permanente la surveillance d'un boîtier HP BladeSystem c-Class, supprimez le boîtier de la console Insight RS. Pour supprimer le boîtier, sélectionnez-le dans l'onglet **Device Summary**, puis sélectionnez **ACTIONS>DELETE SELECTED**.

   La désactivation ou la suppression du boîtier de la console Insight RS ne désinscrit pas le boîtier dans le module OA. Pour que le module OA sache qu'un boîtier est désactivé, vous devez utiliser le module OA pour le désinscrire de Insight Remote Support.
3. Accédez à la page **Enclosure Information>Enclosure Settings>Remote Support**.

4. cliquez sur **Désinscription** ;

   Le message suivant apparaît : `Are you sure you want to un-register and disable HP Insight Remote Support?`.

5. Cliquez sur **OK**.

   Le message suivant s'affiche : `The enclosure is not registered` (Le boîtier n'est pas inscrit).

Erreur de connexion lors de l'inscription à OA direct connect

Problème : L'erreur suivante se produit lorsque vous essayez d'inscrire un boîtier HP BladeSystem c-Class pour Insight Online direct connect :

```
Failed to connect to HP Insight Remote Support direct connect web
service. (Échec de connexion au service Web de connexion directe de
HP Insight Remote Support.) Please verify DNS settings, proxy settings
and connectivity. (Vérifiez les paramètres DNS, les paramètres du proxy
et la connectivité.)
```

Solution 1 : Vérifiez que les paramètres DNS sont correctement configurés dans OA. Vous pouvez utiliser l'interface Web ou CLI de OA pour exécuter cette tâche :

- Connectez-vous à l'interface Web OA et accédez à l'écran **Active Onboard Administrator TCP/IP Settings** (Écran TCP/IP Settings du module Onboard Administrator actif à la page 211). Vérifiez que la configuration DNS est correcte. Pour modifier la configuration, cliquez sur le lien suivant au bas de l'écran : **Click here to modify the TCP/IP settings** (Cliquez ici pour modifier les paramètres TCP/IP).
- Connectez-vous à l'interface CLI de OA et exécutez la commande `SHOW NETWORK`. Vérifiez que la configuration DNS est correcte. Pour modifier la configuration, utilisez la commande `ADD OA DNS`.

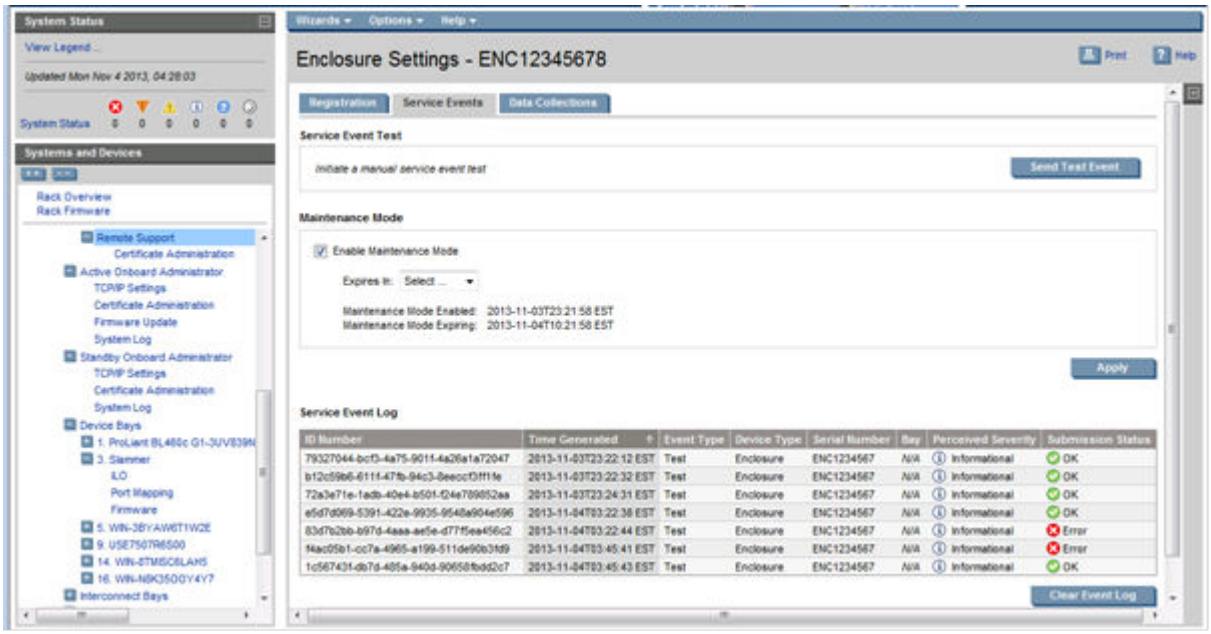
Solution 2 : Vérifiez que les paramètres de proxy Web sont correctement configurés dans OA.

Solution 3 : Vérifiez que votre configuration est conforme aux exigences réseau pour Insight Online direct connect.

Erreur de connexion pendant l'inscription ou la désinscription, ou après l'inscription

Si, au cours du processus d'inscription ou de désinscription ou après l'inscription, une erreur de connexion se produit entre le module Onboard Administrator et Insight Remote Support central connect ou Insight Online direct connect, une interruption SNMP est générée pour indiquer cette défaillance.

Événements de service Insight Remote Support



Utilisez la page Remote Support Service Events pour surveiller les événements de service, envoyer des événements de test ou définir le mode de maintenance.

Un événement de service est une défaillance matérielle, par exemple, un problème lié à un module d'alimentation de boîtier ou un module de ventilation de boîtier. Lorsque le boîtier BladeSystem Enclosure est inscrit à l'aide de Insight Remote Support, des événements de service sont consignés et envoyés à HP. Lorsque HP reçoit un événement de service, une demande d'assistance est ouverte et les détails sont affichés dans le journal des événements de service.

REMARQUE : Pour recevoir des alertes électroniques sur les événements du système, configurez AlertMail sur la page **Enclosure Information>Enclosure Settings>AlertMail**.

Utilisation du mode de maintenance

Utilisez le mode de maintenance lors de l'entretien d'un système. Au cours de cette période, si un événement de service est généré, l'événement indique que le système est en mode de maintenance. Cet événement de service permet à HP de déterminer s'il y a lieu d'ouvrir une demande d'assistance. Si le mode de maintenance n'est pas désactivé par l'utilisateur explicitement pendant cette période, il est automatiquement désactivé par le module Onboard Administrator après l'expiration de la durée de temps sélectionnée.

Pour utiliser le mode de maintenance :

1. Cochez la case **Enable Maintenance Mode** (Activer mode de maintenance).
2. Sélectionnez une durée dans le menu **Expires in** (Expire dans).
3. Cliquez sur **Apply** (Appliquer).

Le mode de maintenance se désactive automatiquement lorsque la durée de temps choisie s'est écoulée.

ASTUCE : Pour mettre fin prématurément au mode de maintenance, désactivez la case **Enable Maintenance Mode**, puis cliquez sur **Apply** (Appliquer).

Envoi d'un événement de service de test

Pour vérifier que votre configuration Insight Remote Support est correcte, cliquez sur **Send Test Event** pour envoyer un événement de test.

Une fois la transmission terminée, l'événement de test est répertorié dans le journal des événements de service.

Affichage du journal des événements de service

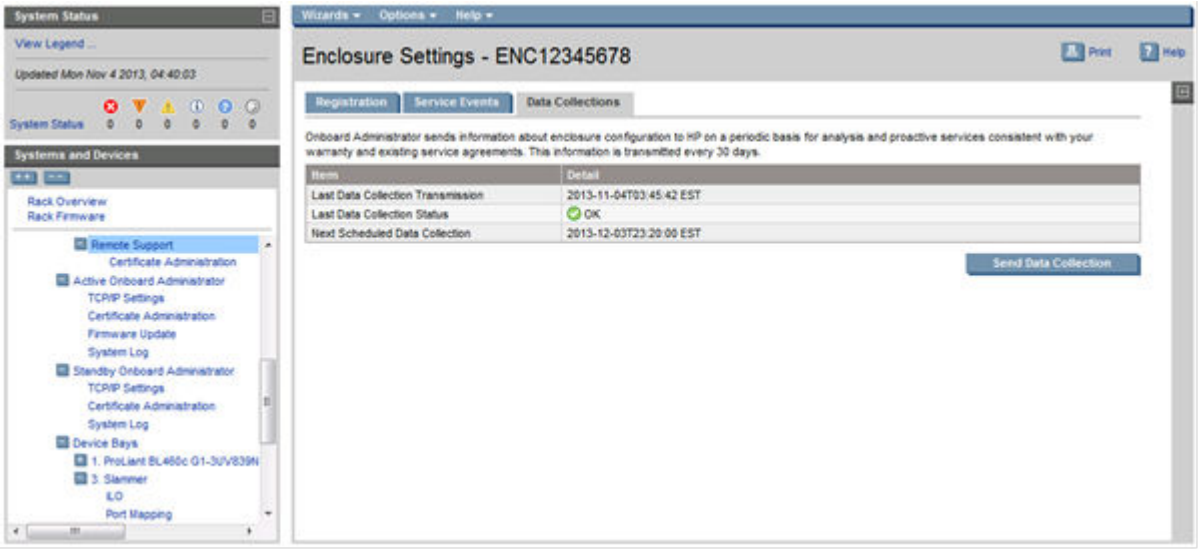
Le journal des événements de service affiche les informations suivantes pour chaque événement de service.

Rangée	Description
ID Number (Numéro ID)	Chaîne unique qui identifie l'événement de service.
Time Generated (Heure de génération)	Heure à laquelle l'événement de service a été généré.
Event Type (Type d'événement)	Chaque événement est classé avec un type : système ou test.
Device Type (Type de périphérique)	Chaîne qui identifie la source de l'événement. Les valeurs possibles sont Fan (Ventilateur), Power Supply (Alimentation), Onboard Administrator, Interconnect (Interconnexion) ou Enclosure (Boîtier).
Serial Number (Numéro de série)	Chaîne qui fournit le numéro de série du périphérique qui a généré l'événement.
Bay (Baie)	Numéro de la baie du périphérique qui a généré l'événement.
Perceived Severity (Gravité perçue)	Chaîne qui indique la gravité de l'événement. Les valeurs possibles sont Critical Error (Erreur critique), Degraded (Dégradé) ou Informational (Informationnel).
Submission Status (État de soumission)	État de la soumission de l'événement. Les valeurs possibles sont OK et ERROR.

Effacement du journal des événements de service

Pour effacer le journal des événements de services, cliquez sur **Clear Event Log**.

Collectes de données Insight Remote Support



Informations de collecte de données

HP Insight Online direct connect

Rangée	Description
Last Data Collection Transmission (Transmission de la dernière collecte de données)	Date et heure de la dernière collecte de données réussie
Last Data Collection Status (État de la dernière collecte de données)	L'état de la transmission ; les valeurs possibles sont OK ou Error
Next Scheduled Data Collection (Prochaine collecte de données planifiée)	La date et l'heure de la prochaine collecte de données programmée, la collecte de données est prévue automatiquement à intervalles de 30 jours

HP Insight Remote Support

Rangée	Description
Last Data Collection Transmission (Transmission de la dernière collecte de données)	Date et heure de la dernière collecte de données réussie
Last Data Collection Status (État de la dernière collecte de données)	L'état de la transmission ; les valeurs possibles sont OK ou Error

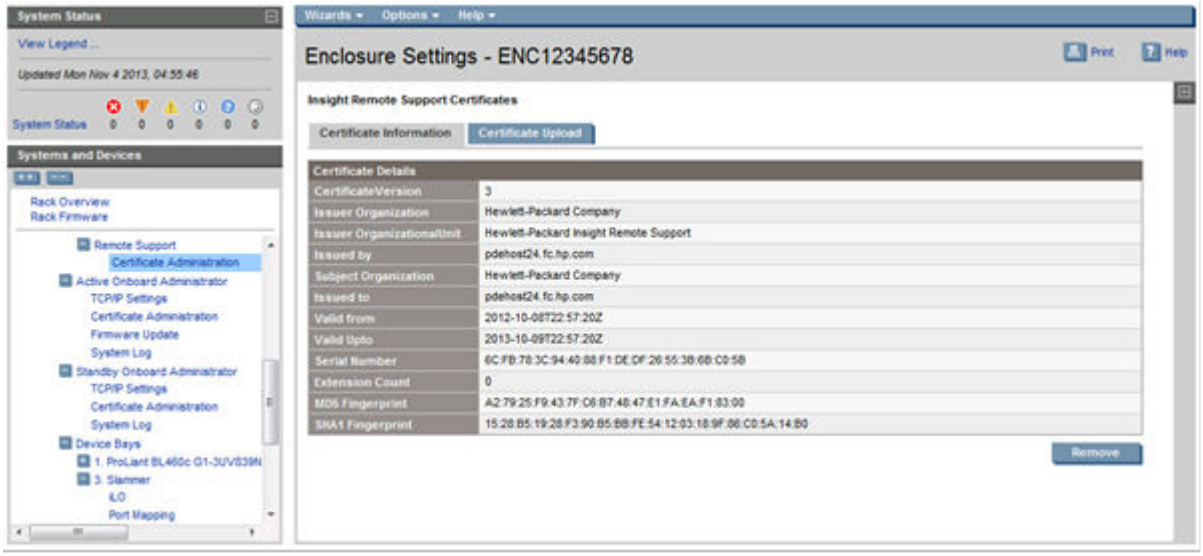
Pour envoyer immédiatement la collecte de données à HP, cliquez sur **Send Data Collection**. Vous devez disposer des droits d'administrateur pour effectuer cette tâche.

Rubriques connexes

Inscription à Insight Remote Support (Inscription à Insight Remote Support à la page 183)

Événements de service Insight Remote Support (Événements de service Insight Remote Support à la page 190)

Administration de certificat de Remote Support



Onglet Certificate Information

Cet écran affiche tous les certificats du serveur Insight Remote Support approuvés par le module Onboard Administrator. Huit certificats au maximum peuvent être téléchargés vers le module Onboard Administrator. Les certificats garantissent que le module Onboard Administrator envoie des informations en toute sécurité vers le serveur Insight Remote Control. Si aucun certificat n'est utilisé, la communication est vulnérable à une attaque d'intercepteur (man-in-the-middle). Pour vous assurer que le certificat est valide et qu'il n'a pas été modifié, vérifiez l'empreinte SHA1 du certificat par une méthode distincte, comme le courrier électronique de l'administrateur du serveur, une page Web ou une autre source fiable.

REMARQUE : Un certificat valide est requis en cas de connexion à un périphérique d'hébergement HP Insight Remote Support et si le module Onboard Administrator fonctionne en mode FIPS.

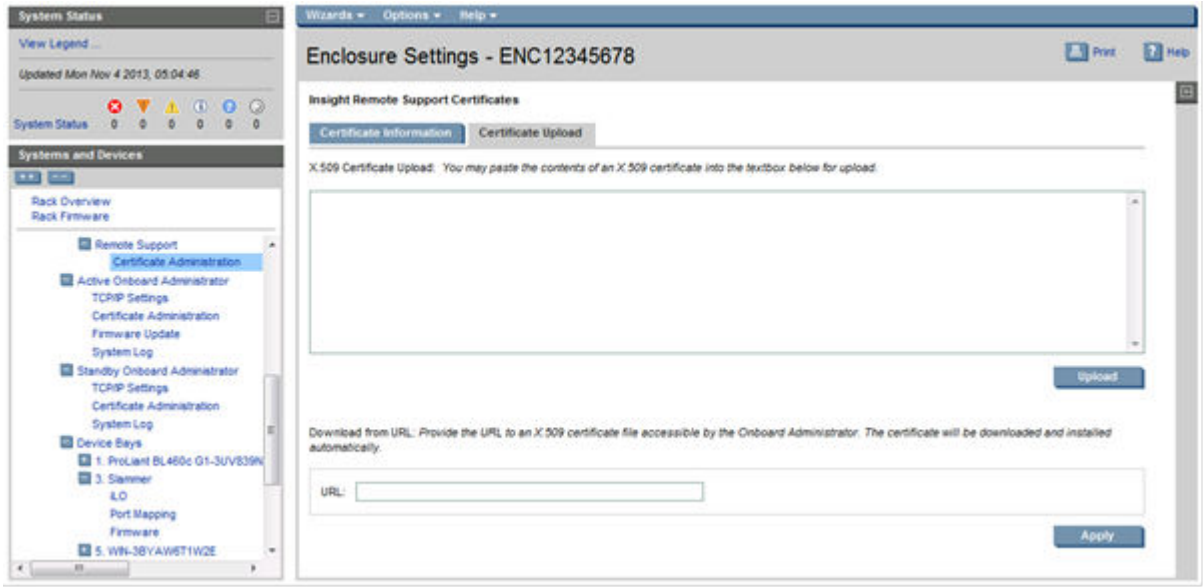
REMARQUE : Lorsque le module Onboard Administrator fonctionne en mode FIPS, la longueur minimale de la clé RSA ne doit pas être inférieure à 2 048 bits, et l'algorithme de hachage de la signature doit être SHA1, SHA-224, SHA-256, SHA-384 ou SHA-512.

Rangée	Description
Certificate Version (Version du certificat)	Numéro de version du certificat actuel
Issuer Organization (Organisation émettrice)	Nom de l'organisation qui a émis le certificat
Issuer Organization Unit (Unité de l'organisation émettrice)	Nom de l'unité organisationnelle qui a émis le certificat
Issued by (Émis par)	Autorité de certification qui a émis le certificat
Subject Organization (Organisation d'objet)	Nom de l'objet
Issued To (Émis à)	Organisation à laquelle le certificat a été émis
Valid From (Valide à partir de)	Date à partir de laquelle le certificat est valide
Valid Upto (Valide jusqu'à)	Date à laquelle le certificat expire
Serial Number (Numéro de série)	Numéro de série attribué au certificat par l'autorité de certification
Extension Count (Nombre d'extensions)	Nombre d'extensions dans le certificat

Rangée	Description
MD5 Fingerprint (Empreinte MD5)	Ce champ peut être utilisé pour valider l'authenticité du certificat
SHA1 Fingerprint (Empreinte SHA1)	Ce champ peut être utilisé pour valider l'authenticité du certificat.

Pour supprimer un certificat existant, cliquez sur **Remove**.

Onglet Support Certificate Administration Upload de Remote Support



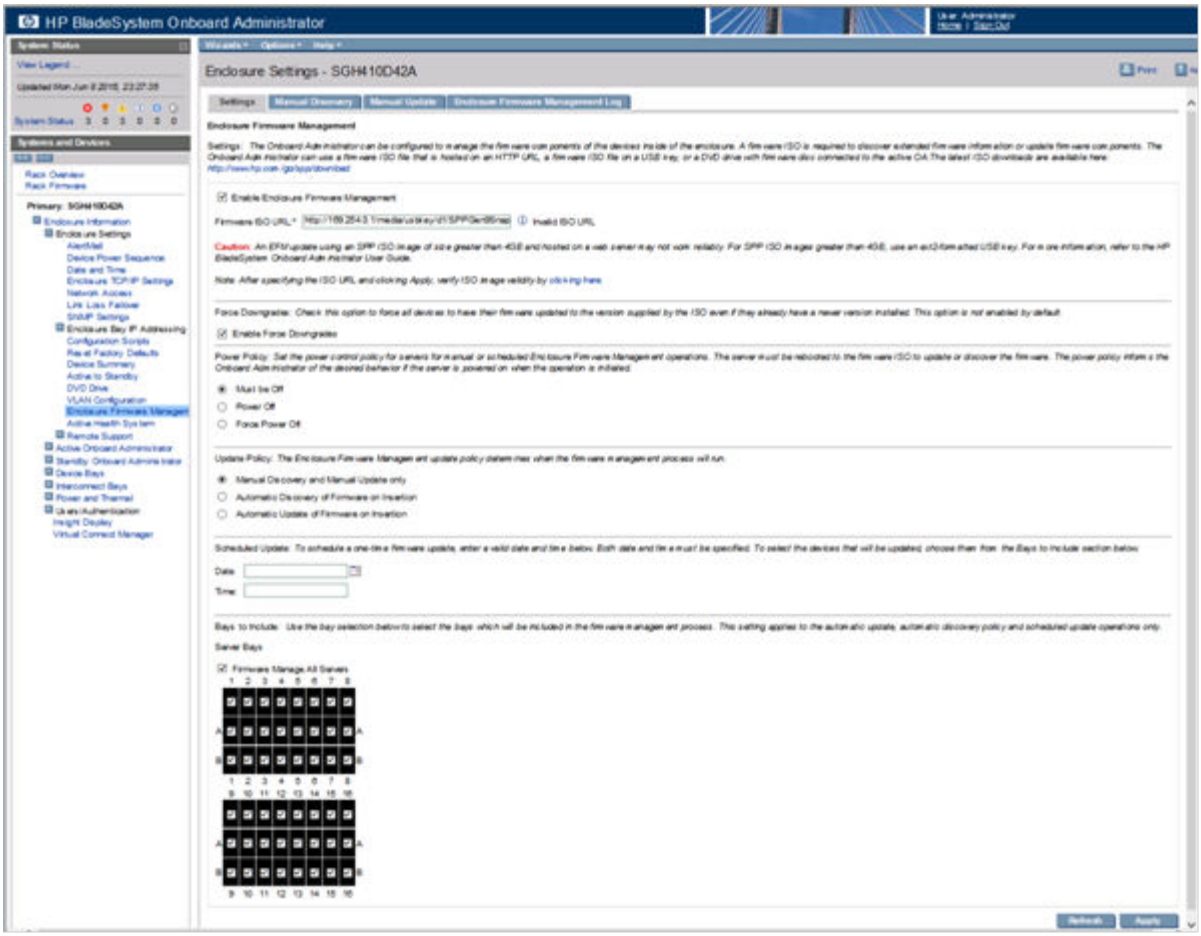
Onglet Certificate Upload

Téléchargez le certificat du serveur Insight Remote Support vers le module Onboard Administrator.

Vous pouvez utiliser deux méthodes pour télécharger des certificats en vue de les utiliser dans le module HP BladeSystem Onboard Administrator :

- Collez le contenu du certificat dans la zone de texte et sélectionnez **Upload** (Télécharger).
- Collez l'URL complète du certificat dans le champ URL et sélectionnez **Apply** (Appliquer).

Enclosure Firmware Management



La fonction Enclosure Firmware Management fournit un point unique à partir duquel gérer des microprogrammes sur des serveurs HP pris en charge et des modules d'interconnexion dans le boîtier. En conséquence, EFM permet aux administrateurs de définir une référence de microprogramme unique (version du SPP) pour les lames de serveur dans un boîtier. Le microprogramme peut être mis à jour à la référence lors de l'insertion du serveur ou au cours d'une période de maintenance pré-définie, ou le microprogramme peut être mis à jour manuellement. Le module Onboard Administrator assure la maintenance des journaux de mises à jour de microprogrammes EFM et des rapports de conformité avec la référence établie.

Exécution de la fonction Enclosure Firmware Management et génération de rapports

Au cours d'une mise à jour de microprogramme EFM de périphériques dans le boîtier, les différentes phases du processus de mise à jour et du traitement associé qui s'exécutent sur le module OA consomment une quantité importante de ressources du module OA (processeur, mémoire et débit réseau). Cela est valable surtout lorsque vous tentez d'effectuer la mise à jour du microprogramme de plusieurs lames simultanément dans le boîtier. Les ressources dans le module OA peuvent ne pas être suffisantes pour prendre en charge la mise à jour simultanée du microprogramme de tous les périphériques dans un boîtier. Par conséquent, il est nécessaire de contrôler les demandes de charge ponctuelles que le traitement EFM place sur le module OA. Pour ce faire, le microprogramme OA met en œuvre un type de contrôle des tâches basé sur une heuristique dynamique de gestion de ressources qui tente de limiter l'utilisation des ressources du traitement lié à la fonction EFM à un niveau qui n'interfère pas avec la capacité du module OA pour effectuer ses autres tâches de gestion du boîtier. Dans le cadre de cette heuristique dynamique de gestion des ressources, le microprogramme OA surveille spécifiquement les facteurs suivants :

- Utilisation des processeurs (plus spécifiquement, la moyenne des charges de processus du processeur intégré au module OA)
- Utilisation de la mémoire
- Nombre de transferts en attente de l'image ISO des microprogrammes vers les lames via le support virtuel iLO.

En fonction de ces facteurs, la logique de contrôle des tâches EFM met à jour les serveurs par lots lorsque cela est nécessaire en (1) autorisant la mise à jour simultanée d'autant de périphériques dans le boîtier qui peuvent être placés dans les limites des ressources établies appliquées par la heuristique dynamique de gestion de ressources et en (2) retardant la mise à jour d'autres périphériques jusqu'à ce que des ressources deviennent disponibles. Par conséquent, lorsque la mise à jour simultanée de plusieurs périphériques de boîtier est tentée, certaines de toutes les mises à jour peuvent ne pas être effectuées en même temps. Le point auquel l'exécution par lots se produit est variable et dépend de plusieurs facteurs : le nombre de périphériques sélectionnés pour la mise à jour, des considérations relatives à la gestion réseau telles que la quantité et le type de trafic, la configuration spécifique au module OA, d'autres activités de gestion en suspens effectuées par le module OA, ainsi que tout autre facteur qui a une incidence sur l'utilisation des ressources sur le module OA lorsque la mise à jour EFM est initiée. La preuve d'une telle exécution par lots peut se révéler dans certains délais indiqués dans le journal des microprogrammes.

Pour plus d'informations sur le journal des microprogrammes et tout autre journal de gestion de microprogramme, consultez la section « Journaux de gestion des microprogrammes » (Journaux de gestion des microprogrammes à la page 280).

EFM et intégration avec HP SUM

EFM détecte et met à jour le microprogramme en démarrant un serveur à partir d'une image ISO du HP SPP pris en charge. EFM orchestre le moteur HP SUM intégré dans l'image ISO de SPP, ce qui fournit des résultats comparables à une exécution manuelle de HP SUM, mais ce qui permet de gagner du temps en centralisant le contrôle et en détection et en mettant à jour le microprogramme sur plusieurs serveurs.

Au cours de l'exécution d'une tâche EFM, si une opération de HP SUM ou EFM associée échoue, EFM lance automatiquement une nouvelle tentative de la tâche EFM entière. EFM tentera d'exécuter la tâche trois fois au total. Les tentatives effectuées répètent potentiellement des étapes déjà réalisées dans la tâche EFM, selon le point où l'échec se produit. Si la tâche ne peut pas être effectuée avec succès au cours de la dernière tentative, la tâche EFM se termine avec un état d'échec.

REMARQUE : Dans de rares circonstances, bien que les processus de HP SUM se terminent avec un état d'échec, des journaux EFM peuvent toujours indiquer une réussite de la tâche EFM globale. Des niveaux de microprogramme ne seront pas mis à jour comme prévu, et ceci peut être observé par une incohérence entre les versions de microprogramme installées indiquées et les versions de microprogramme disponibles sur l'image ISO de microprogramme utilisée. Lorsqu'une incohérence de ce type se produit, HP recommande de rechercher dans les journaux du microprogramme et de la session des preuves d'un échec de HP SUM. Si un tel échec est indiqué, la tâche EFM peut avoir également échoué. Pour plus d'informations sur les journaux EFM, consultez la section « Journaux de gestion des microprogramme » (Journaux de gestion des microprogrammes à la page 280). Pour plus d'informations sur les échecs EFM, consultez la section « Journal Enclosure Firmware Management » (Journal Enclosure Firmware Management à la page 203). Pour plus d'informations sur l'affichage des versions de microprogramme, consultez la section « Affichage des versions de microprogramme » (Affichage des versions des microprogrammes à la page 282).

Autres précautions relatives aux performances de traitement

La fonction Enclosure Firmware Management ne fonctionnera pas de manière fiable et ne doit pas être utilisée sur des liaisons de réseau lentes (inférieures à 1 Go).

Pendant l'exécution d'opérations Enclosure Firmware Management, le temps de réponse du module Onboard Administrator peut être plus lent que d'habitude et lors de brefs intervalles, l'état du boîtier peut être signalé comme étant détérioré. Vous pouvez ignorer les messages ou des conditions d'alerte de cette nature tandis que les opérations sont en cours.

REMARQUE : Les performances de la fonctionnalité de support virtuel iLO Integrity et HP c-Class BladeSystem ProLiant seront limitées par l'activité et le nombre de sessions simultanées de support virtuel iLO et la charge de travail Onboard Administrator. Les fonctionnalités Enclosure Firmware Management et de DVD de boîtier Onboard Administrator utilisent également la fonction de support virtuel iLO et auront des restrictions de performances similaires. Pour éviter les problèmes de délai d'attente de support, HP recommande de limiter le nombre de sessions simultanées. Si des problèmes de délai d'attente sont rencontrés au cours d'une installation de système d'exploitation ou de mises à jour de microprogramme, réduisez le nombre de sessions de support virtuel en cours et redémarrez l'opération.

REMARQUE : Dans de rares cas au cours d'une tâche EFM, certains échecs du côté serveur (par exemple, le processus de mise à jour du microprogramme iLO se bloque ou son exécution prend un temps excessif) peuvent se produire sans fournir d'indications d'échec au processus EFM associé. Lorsque de telles erreurs se produisent, la tâche EFM du module OA ne se termine pas et semble être bloquée avec aucun état ou avancement signalé. Pour récupérer à partir de cette condition, redémarrez le module OA actif ou effectuez un basculement manuel vers le module OA redondant.

Paramètres de l'utilitaire Enclosure Firmware Management

Les paramètres Enclosure Firmware Management sont réservés aux utilisateurs du module Onboard Administrator dotés de droits d'administrateur et sont accessibles sur l'interface utilisateur du module Onboard Administrator à la page **Enclosure Settings>Enclosure Firmware Management** ou à partir de la ligne de commande du module Onboard Administrator.

Autorisations utilisateur obligatoires

Toutes les fonctions Enclosure Firmware Management sont disponibles via l'interface CLI et l'interface du module Onboard Administrator, sauf si Secure Boot est en vigueur pour la lame dans le boîtier. Le mode Secure Boot empêche les utilisateurs de modifier des options de démarrage ou d'effectuer des opérations de démarrage à partir de l'interface CLI ou l'interface utilisateur du module Onboard Administrator. Ces tâches doivent être effectuées à partir du périphérique configuré dans le BIOS par l'administrateur.

Les rôles utilisateur et les autorisations de baie du module Onboard Administrator contrôlent les paramètres de l'utilitaire Enclosure Firmware Management et la possibilité de voir les informations relatives aux microprogrammes.

Rôle utilisateur	Modifier des paramètres ou des mises à jour programmées	Initier des détections ou mises à jour manuelles	Afficher les versions des microprogrammes
Administrateur ou opérateur du module Onboard Administrator	Oui	Oui, administrateur OA uniquement*	Oui
Administrateur ou opérateur du serveur	Non	Oui, administrateur OA uniquement*	Oui, autorisé pour les baies de serveur

Rôle utilisateur	Modifier des paramètres ou des mises à jour programmées	Initier des détections ou mises à jour manuelles	Afficher les versions des microprogrammes
Utilisateur du module Onboard Administrator	Non	Non	Oui, autorisé pour les baies

* Si le mode Secure Boot est en vigueur pour la lame dans le boîtier, cette opération ne peut pas être effectuée à partir de l'interface CLI ou de l'utilisateur.

Enabling Enclosure Firmware Management

La case à cocher **Enable Enclosure Firmware Management** permet d'activer ou de désactiver globalement (paramètre par défaut) l'utilitaire Enclosure Firmware Management. Lorsqu'elle n'est pas cochée, il est impossible de lancer une opération manuelle de gestion des microprogrammes. Toute opération antérieurement configurée automatiquement ou programmée n'est pas effectuée. Si le paramètre passe de l'état activé à l'état désactivé, toutes les opérations en cours de détection ou de mise à jour de l'utilitaire Enclosure Firmware Management sont d'abord terminées.

REMARQUE : Une fois lancées, les opérations Enclosure Firmware Management (mises à jour et détections) ne peuvent pas être interrompues. Assurez-vous que votre boîtier est activé IPv6 avant d'utiliser une adresse IPv6 de l'ISO de gestion des microprogrammes.

L'utilitaire Enclosure Firmware Management n'est pas pris en charge sur les modules matériels Onboard Administrator suivants :

- HP BladeSystem c3000 Onboard Administrator (numéro de référence HP 448589-B21, 461514-B21)
- HP BladeSystem c7000 Onboard Administrator (numéro de référence HP 412142-B21)

La fonction Enclosure Firmware Management ne peut être activée que si le module matériel Onboard Administrator actif est pris en charge. Si vous tentez d'activer la fonction Enclosure Firmware Management alors que le module Onboard Administrator n'est pas pris en charge, un message d'erreur s'affiche :

```
Enclosure Firmware Management is not supported on the active OA hardware
present.
```

Si le module Onboard Administrator en Standby n'est pas pris en charge, un message d'avertissement s'affiche :

```
Enclosure Firmware Management is not supported on the standby OA hardware
present. The feature will be disabled if the standby OA becomes Active.
```

L'utilitaire Enclosure Firmware Management échoue sur toute lame si SSH est désactivé dans les paramètres de configuration iLO de la lame. Par défaut, SSH est activé dans iLO.

Configuration de l'emplacement de l'image des microprogrammes

Pour effectuer la détection ou des mises à jour de microprogramme, l'utilitaire Enclosure Firmware Management nécessite une image ISO de microprogramme. Les images ISO les plus récentes sont disponibles pour téléchargement à partir du site Web HP (http://www.hp.com/go/spp/download).

Vous pouvez fournir un des emplacements suivants pour l'image ISO du microprogramme :

- Une image ISO HTTP basée sur une URL et hébergée sur un serveur Web. Fournissez une adresse IPv4 dans le format suivant : `protocole://[<Adresse_IPv4>]/chemin/nom_fichier`. Pour fournir une adresse IPv6 basée sur une URL, spécifiez l'adresse entre

parenthèses dans le format suivant : `protocole://[<Adresse_IPv6>]/chemin/nom_fichier`.

La longueur maximum de l'URL est de 511 caractères.

La taille maximale prise en charge de l'image ISO de SPP est de 4 Go. Avec des images ISO de SPP de taille supérieure à 4 Go, créez une image ISO personnalisée qui exclut les composants inutiles pour le processus de mise à jour du microprogramme de lame OA EFM. L'image ISO personnalisée doit contenir au minimum les composants de microprogramme pour les lames de serveur HP ProLiant BL Series. Pour plus d'informations sur la création d'une image ISO personnalisée, consultez le *Manuel de l'utilisateur du module HP BladeSystem Onboard Administrator*.

Pour utiliser la totalité de l'image ISO avec une taille de fichier supérieure à 4 Go, vous devez disposer d'une clé USB au format ext2.

- Une clé USB contenant l'image ISO connectée au port USB du module Onboard Administrator.

  Une clé USB convertie en support amorçable à partir de l'image ISO fr SPP n'est pas prise en charge par l'utilitaire Enclosure Firmware Management. L'image ISO doit se trouver dans le répertoire racine de la clé USB.

  La taille maximale de fichier prise en charge pour les clés USB formatées avec FAT32 est de 4 Go. Pour les images SPP supérieures à 4 Go, utilisez une clé USB de format ext2. Pour plus d'informations sur le formatage d'une clé USB avec un système de fichiers ext2, consultez la section « Écran USB Menu » (Écran USB Menu à la page 43).

- Un DVD physique inséré dans le lecteur de DVD du boîtier. Lors de l'utilisation d'un DVD physique, le DVD ne doit pas contenir l'image ISO. Ce dernier doit être un disque amorçable créé à partir de l'image ISO.

REMARQUE : Après avoir désactivé IPv6 en vue d'une conversion vers un environnement strictement IPv4, si l'URL de l'image ISO du microprogramme Enclosure Firmware Management spécifie une clé USB ou une URL basée sur IPv6 pour un serveur Web, vous devez saisir de nouveau l'emplacement de la clé USB ou fournir une URL basée sur IPv4 pour le serveur Web. Sinon, EFM ne peut pas accéder à l'image ISO.

REMARQUE : Après avoir spécifié l'URL de l'image ISO et cliqué sur **Apply** (Appliquer), vérifiez la validité de l'image ISO en cliquant sur le lien **clicking here** (Cliquer ici).

Création d'une image ISO de SPP personnalisée

Les instructions suivantes fournissent les étapes de base pour la création d'une image ISO du SPP personnalisée compatible pour la fonction EFM du module Onboard Administrator. Il est supposé que vous avez de l'expérience dans l'utilisation de HP SUM pour la création d'images ISO personnalisées. Pour plus d'informations, reportez-vous à l'aide en ligne de HP SUM, ou consultez le livre blanc *Building and deploying a customized SPP firmware ISO image* (Génération et déploiement d'une image ISO de microprogramme SPP personnalisée), ainsi que d'autres documents de la bibliothèque HP Enterprise (http://www.hp.com/go/hpsum/documentation).

1. Téléchargez l'image ISO du SPP contenant HP SUM 7.2 (ou version ultérieure) vers un dossier sur votre disque local.
2. Lancez le fichier de traitement par lots de HP SUM.
3. Dans le menu **Options**, sélectionnez **Baseline Library** (Bibliothèque de références). Le SPP est automatiquement ajouté en tant que référence. Avant de procéder à l'étape suivante, attendez que HP SUM s'affiche et termine l'inventaire sur la référence.
4. À partir de l'onglet **Actions** de la fenêtre Baseline Library, sélectionnez **Create Custom**.

5. À partir de la fenêtre Create Custom Baseline, spécifiez les informations nécessaires dans la section **Overview**.
   - Pour le champ **Output Location**, spécifiez ou accédez à l'emplacement dans lequel placer l'image ISO personnalisée.
   - Pour le champ **Extracted Source ISO Location**, cliquez sur **Browse** pour sélectionner l'image ISO du SPP source qui sera personnalisée.
   - Cochez la case **Make Bootable ISO file**.
6. Dans la section **Step 2 - Filters** :
   a. Pour le champ **Component Type**, sélectionnez **Firmware**.
   b. Sélectionnez toutes les cases à cocher : **Critical Updates** (Mises à jour critiques), **Recommended Updates** (Mises à jour recommandées) et **Optional Updates** (Mises à jour facultatives).
7. Cliquez sur **Advanced Filters** et sélectionnez les filtres requis.

   Pour le champ **Server Model**, sélectionnez **HP ProLiant BL Series**.
8. Dans la section **Step 3 - Review**, cliquez sur **Apply Filters**.

   Attendez que tous les composants filtrés soient récupérés. L'état de la procédure de récupération peut être visualisé en bas de la page. Une fois le processus terminé, le message `Completed retrieving components` s'affiche.
9. Cliquez sur Create ISO (Créer image ISO).

Après quelques minutes, l'image ISO du SPP personnalisée est prête à être utilisée à l'emplacement **Output Location** spécifié plus haut.

Enabling force downgrades

Cette case à cocher permet d'activer ou de désactiver (paramètre par défaut) le passage forcé à la version antérieure. Lorsqu'elle n'est pas cochée, les composants dotés d'une version de microprogramme supérieure à celle de l'image ISO sont exclus de la mise à jour. Ce paramètre s'applique à toutes les lames de serveur prises en charge dans ce boîtier. Lorsque la case n'est pas cochée, l'utilitaire Enclosure Firmware Management commande au moteur HP SUM de flasher les microprogrammes du composant dont la version est ultérieure à celle de l'image. L'activation de ce paramètre ne garantit pas la rétrogradation du microprogramme à une version antérieure. Si vous utilisez l'option Enable Force Downgrades (Activer le passage forcé à la version antérieure), veillez à consulter la documentation ISO pour assurer le réglage approprié du paramètre.

Définition de la politique de l'alimentation

Pour être en mesure de mettre à jour ou de détecter les microprogrammes, le serveur doit être initialisé à partir de l'image ISO. La politique en matière d'alimentation informe le module Onboard Administrator de l'action à effectuer si le serveur est mis sous tension lorsque l'opération a débuté. Ce paramètre s'applique aux opérations programmées comme aux opérations manuelles. La politique d'alimentation par défaut est **Must be Off** (Doit être hors tension).

Si la politique d'alimentation est définie sur Power Off (Mettre hors tension), le module Onboard Administrator attend cinq minutes avant de répondre à la demande. Si le serveur ne s'arrête pas au cours de ce laps de temps, l'opération de gestion des microprogrammes échoue. Si le système d'exploitation du serveur a initié l'arrêt mais que le serveur ne s'est pas arrêté dans les cinq minutes, ce dernier peut s'arrêter et rester sous tension.

Paramètre	Description
Must be Off (Doit être hors tension)	Le module Onboard Administrator annule l'opération si le serveur est sous tension.
Power Off (Mettre hors tension)	Le module Onboard Administrator imite une pression momentanée physique du bouton d'alimentation de la lame de serveur, mettant ainsi la lame de serveur hors tension de manière ordonnée.
Force Power Off (Forcer la mise hors tension)	Le module Onboard Administrator imite une pression physique et un maintien enfoncé du bouton d'alimentation de la lame de serveur, forçant ainsi la mise hors tension de la lame de serveur sans mise hors tension préalable du système d'exploitation.

⚠ **ATTENTION :** L'utilisation de la politique Force Power Off (Forcer la mise hors tension) sur les serveurs dotés d'un système d'exploitation exige une certaine prudence, car des données peuvent être endommagées.

Définition de la politique de mise à jour

Les politiques de mise à jour disponibles pour la gestion des microprogrammes comprennent :

- Détection manuelle et mise à jour manuelle uniquement : la politique par défaut. Cette politique empêche le module Onboard Administrator de procéder automatiquement à des mises à jour du serveur ou à des détections au moment de l'insertion dans le boîtier.

  Pour que le module Onboard Administrator soit en mesure d'afficher dans le détail les versions des microprogrammes du serveur, il est nécessaire d'effectuer des opérations de détection ou mise à jour manuelle et de mise à jour programmée.

- Détection automatique au moment de l'insertion : permet au module Onboard Administrator d'effectuer une opération de détection au démarrage sur un serveur activé à l'aide de l'option Baies à inclure. Le module collecte alors des informations détaillées relatives aux microprogrammes pour ce serveur, met à jour le journal de gestion des microprogrammes pour cet événement, puis redémarre le serveur pour reprendre un fonctionnement normal. Vous pouvez alors voir les versions des microprogrammes détectés et mettre ces derniers à jour via une mise à jour manuelle ou programmée.

- Mise à jour automatique au moment de l'insertion : permet au module Onboard Administrator d'effectuer une opération de mise à jour au démarrage sur un serveur activé à l'aide de l'option Baies à inclure. Le module collecte alors des informations détaillées relatives aux microprogrammes mis à jour pour ce serveur, met à jour le journal de gestion des microprogrammes pour cet événement, puis redémarre le serveur pour reprendre un fonctionnement normal. Cette politique permet de mettre à jour les microprogrammes du serveur en fonction de l'image de microprogramme sélectionnée, après un événement de maintenance tel que le remplacement de la carte du serveur ou de la carte en option.

Les politiques de détection automatique et de mise à jour automatique s'excluent mutuellement et s'appliquent à toutes les baies à inclure dans le boîtier.

Définition d'une mise à jour de microprogramme programmée

La politique de mise à jour programmée des microprogrammes indique au module Onboard Administrator la date et l'heure auxquelles mettre automatiquement à jour toutes les baies à inclure aux versions des microprogrammes de l'image ISO des microprogrammes. À la date et à l'heure fixées, le module Onboard Administrator lance une opération de mise à jour à l'aide de la politique d'alimentation sur toutes les baies à inclure, met à jour leurs microprogrammes à l'aide de l'image ISO des microprogrammes, puis redémarre tous les serveurs concernés pour reprendre un fonctionnement normal.

Spécification des baies à inclure dans un processus de gestion du microprogramme

Toutes les baies de périphériques sont incluses par défaut à la gestion des microprogrammes. L'administrateur du module Onboard Administrator peut sélectionner des baies de périphériques spécifiques à inclure et laisser de côté les baies de périphériques non concernées par les politiques de mise à jour, les mises à jour manuelles ou les mises à jour programmées de la gestion des microprogrammes du boîtier.

Par défaut, la case **Firmware Manage All Servers** (Les microprogrammes gèrent tous les serveurs) est cochée et les politiques Enclosure Firmware Management et les mises à jour programmées s'appliquent donc à tous les serveurs disponibles.

Vous pouvez sélectionner séparément toutes les baies de base, baies du côté a et baies du côté b, ou cocher la case **Firmware Manage All Servers** pour sélectionner toutes les baies de périphériques.

Pour sélectionner manuellement des serveurs spécifiques à soumettre à l'utilitaire Enclosure Firmware Management :

1. Décochez la case **Firmware Manage All Servers** (Les microprogrammes gèrent tous les serveurs).
2. Cochez la case en regard de chaque baie à inclure ou sélectionnez les baies selon leur type.
3. Cliquez sur **Apply** (Appliquer). Une liste à jour des baies à inclure pour l'utilitaire Enclosure Firmware Management s'affiche.

Actuellement, seules les baies de périphériques peuvent être sélectionnées. Les travées et les baies du module Onboard Administrator ne sont pas sélectionnables.

L'option de sélection des baies à inclure ne s'applique qu'aux lames de serveur ProLiant. Les lames de serveur Integrity ne prennent pas en charge cette fonctionnalité. La prise en charge des lames partenaires s'effectue via la lame de serveur associée, si l'image ISO des microprogrammes prend en charge la carte adaptateur PCIe dans la lame partenaire.

Journal Enclosure Firmware Management

Pour plus d'informations sur les journaux de microprogramme, y compris le journal Enclosure Firmware Management, consultez la section « Journaux de gestion du microprogramme » (Journaux de gestion des microprogrammes à la page 280).

Détection manuelle

REMARQUE : Lorsqu'une tâche Enclosure Firmware Management est en cours, ne redémarrez pas le module Onboard Administrator. Évitez de mettre la lame hors tension ou de la retirer du boîtier.

Il est possible d'effectuer une opération de détection manuelle sur un ou plusieurs serveurs pour simplifier la collecte des versions des microprogrammes installés.

Lorsqu'on lance une opération manuelle de détection des microprogrammes, un écran de sélection des baies de périphériques s'affiche. Sélectionnez une ou plusieurs baies de périphérique sur lesquelles effectuer la détection ou cochez la case **Discover All Servers** (Détecter tous les serveurs). Toutes les baies de périphériques et la case Discover All Servers sont sélectionnées par défaut.

Si le mode Secure Boot est configuré sur une lame de serveur, vous ne pouvez pas sélectionner la baie associée (une icône de cadenas est affichée). Le mode Secure Boot empêche les utilisateurs d'effectuer une détection manuelle à partir de l'interface CLI ou de l'interface utilisateur du module Onboard Administrator. Les opérations d'amorçage peuvent être effectuées uniquement à partir du périphérique d'amorçage configuré dans le BIOS par l'administrateur.

Pour lancer le processus de découverte sur le serveur sélectionné, cliquez sur **Start Manual Discovery** (Lancer la découverte manuelle).

Mise à jour manuelle

ATTENTION : Il est possible que la mise à jour de Enclosure Firmware Management à l'aide d'une image SPP de taille supérieure à 4 Go et hébergée à partir d'un serveur Web ne fonctionne pas correctement.

REMARQUE : Lorsqu'une tâche Enclosure Firmware Management est en cours, ne redémarrez pas le module Onboard Administrator. Évitez de mettre la lame hors tension ou de la retirer du boîtier.

Une mise à jour manuelle d'un ou de plusieurs serveurs vers les versions d'image des microprogrammes désignées peut être initiée. Pour lancer une mise à jour des microprogrammes sur un ou plusieurs serveurs, cliquez sur **Manual Update** (Mise à jour manuelle).

Lorsqu'on lance une opération manuelle de mise à jour des microprogrammes, un écran de sélection des baies de périphériques s'affiche. Sélectionnez une ou plusieurs baies de périphériques sur lesquelles effectuer la mise à jour ou cochez la case **Update All Servers** (Mettre à jour tous les serveurs) pour sélectionner tous les serveurs pour la mise à jour. Toutes les baies de périphériques et la case Discover All Servers sont sélectionnées par défaut.

Si le mode Secure Boot est configuré sur une lame de serveur, vous ne pouvez pas sélectionner la baie associée (une icône de cadenas est affichée). Le mode Secure Boot empêche les utilisateurs d'effectuer une mise à jour manuelle à partir de l'interface CLI ou de l'interface utilisateur du module Onboard Administrator. Les opérations d'amorçage peuvent être effectuées uniquement à partir du périphérique d'amorçage configuré dans le BIOS par l'administrateur.

Pour lancer le processus de mise à jour sur le serveur sélectionné, cliquez sur **Start Manual Update** (Lancer la mise à jour manuelle).

Journal Enclosure Firmware Management

Le journal Enclosure Firmware Management offre une vue d'ensemble des principaux événements de l'utilitaire Enclosure Firmware Management, tels que les sélections d'images de microprogramme, les modifications programmées ou liées aux politiques et les opérations de microprogramme initiées et terminées. Ce journal ne contient pas les détails inclus dans le journal des microprogrammes pour chaque serveur.

Le journal Enclosure Firmware Management est conservé entre les réamorçages OA et les pertes d'alimentation. Il est conservé sur le module OA en mode Standby, s'il est présent.

Pour visualiser des informations de journal mises à jour, cliquez sur **Refresh** (Actualiser).

Pour effacer les informations concernant le journal Enclosure Firmware Management et le journal des microprogrammes spécifiques au serveur et le journal de session, cliquez sur **Clear All Logs** (Effacer tous les journaux). (Pour plus d'informations sur le journal des microprogrammes et le journal de session, consultez la section « Journaux de gestion du microprogramme » (Journaux de gestion des microprogrammes à la page 280)).

Pour effacer les informations concernant le journal Enclosure Firmware Management, cliquez sur **Clear Log** (Effacer le journal).

ATTENTION : Une fois supprimées, ces données ne peuvent pas être restaurées.

Échecs d'événement

À la fin d'une tâche Enclosure Firmware Management, le dernier événement indiqué sur le journal des microprogrammes du serveur est `Firmware Management successfully completed`

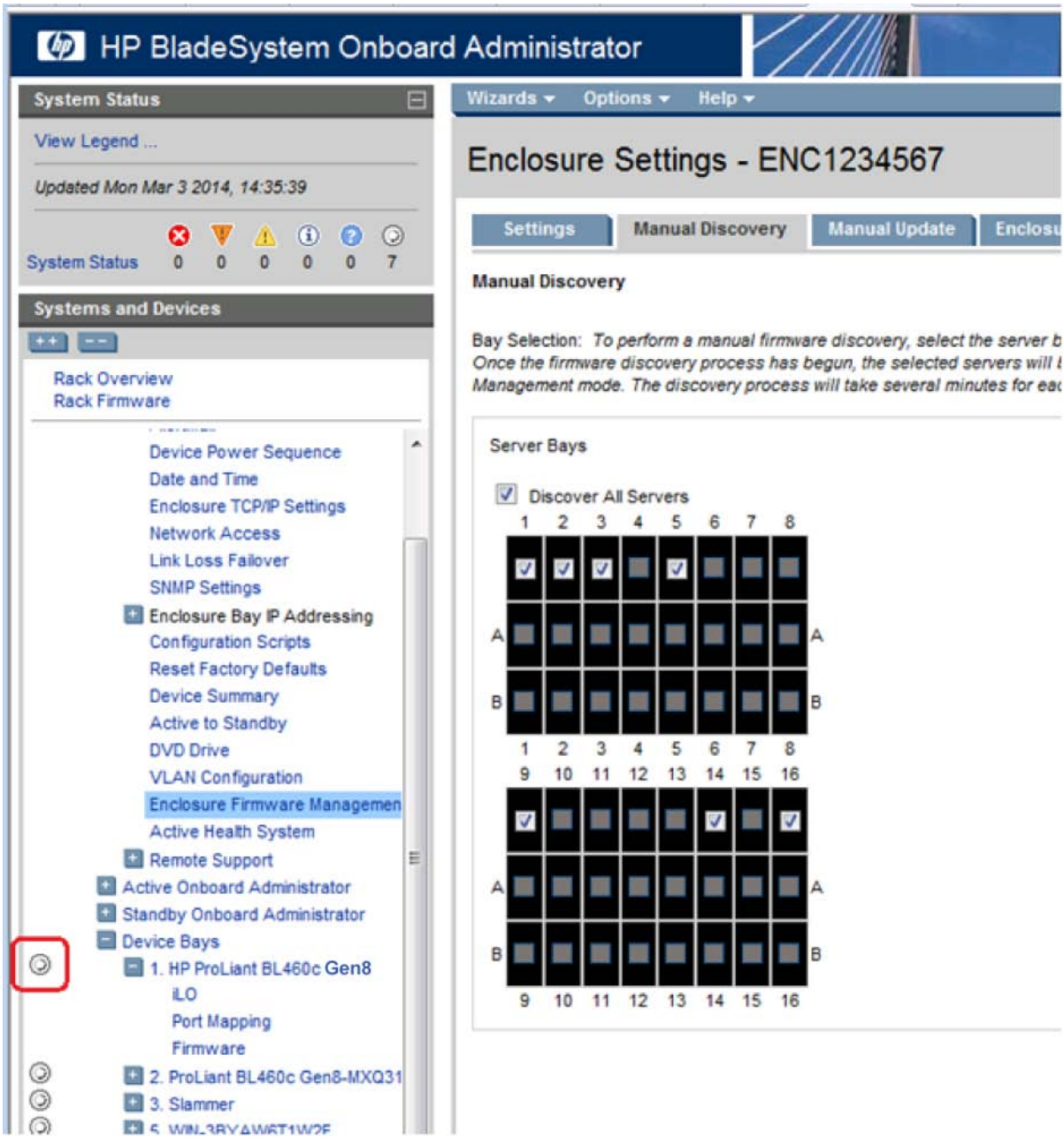
(Gestion des microprogrammes terminée) ou `Firmware Management is incomplete` (Gestion des microprogrammes non terminée).

Si la dernière opération qui apparaît sur le journal Enclosure Firmware Management n'indique pas une réussite, les entrées de l'autre journal des microprogrammes peuvent indiquer le problème rencontré par le module Onboard Administrator. Par exemple, pour effectuer une opération de détection manuelle, une mise à jour manuelle ou une mise à jour programmée, le serveur doit être hors tension. Le journal peut indiquer que le serveur était sous tension et que l'opération de gestion des microprogrammes a donc été interrompue.

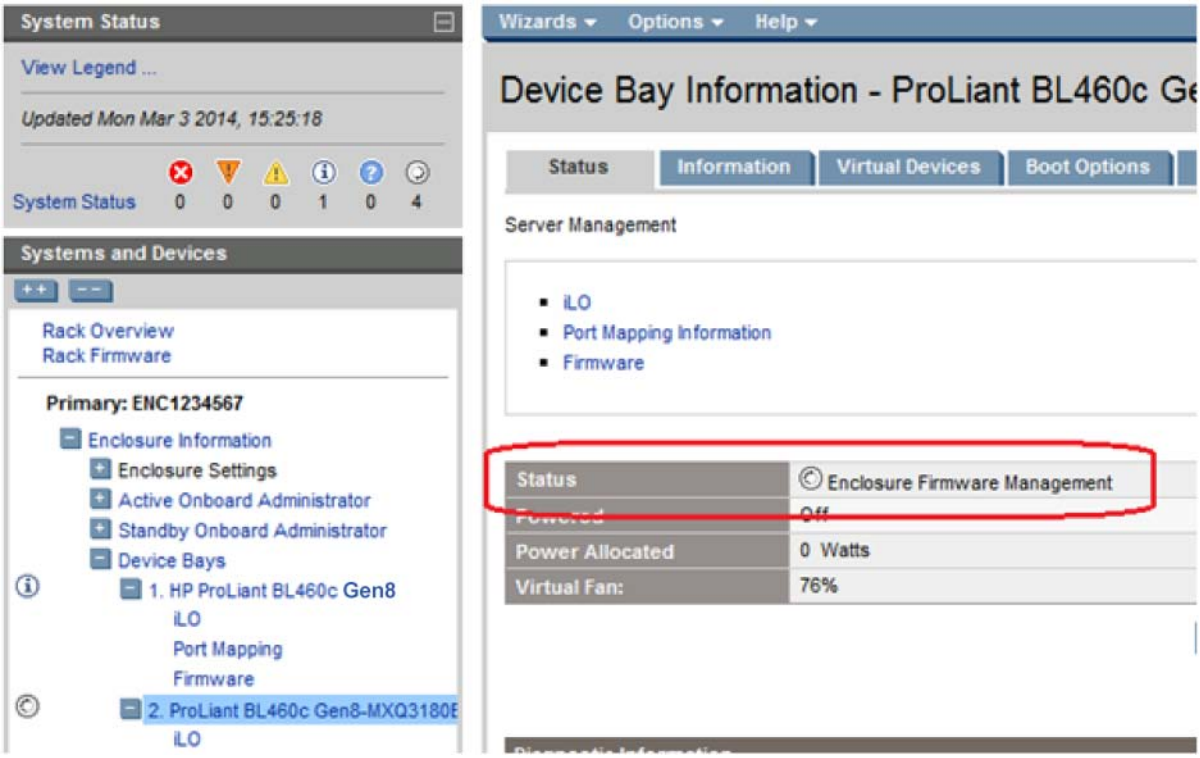
En cas de défaillance lors de la réalisation d'une tâche Enclosure Firmware Management, l'entrée ratée est connectée en tant que `Firmware Management failed on blade X` (Échec de gestion des microprogrammes sur la lame X). Le module Onboard Administrator tente de réaliser à nouveau la tâche jusqu'à trois fois. Si la tâche est menée à bien, les précédentes entrées signalant un échec peuvent être ignorées. Pour obtenir des informations détaillées sur les événements et l'activité en cours, consultez le journal des microprogrammes correspondant au serveur.

Mises à jour d'état

Lorsqu'une tâche Enclosure Firmware Management telle qu'une opération de détection ou de mise à jour manuelle est démarrée sur un serveur, une icône d'état Enclosure Firmware Management s'affiche dans le volet de navigation de gauche à côté de chaque périphérique affecté. Dans la figure suivante, une de plusieurs de ces icônes est encerclée en rouge.



Lorsque la tâche Enclosure Firmware Management est en cours de traitement, l'onglet Device Bay Status (État de baie de périphérique) (Onglet Device Bay Status à la page 240) affiche l'état du serveur en tant que `Firmware Management`, comme indiqué dans la figure suivante.



Une fois la tâche terminée, l'état du serveur est à nouveau illustré par l'icône adéquate. Pour connaître la signification des icônes d'état, cliquez sur **View légende** (Afficher la légende) près du haut du volet de navigation de gauche.

Les informations détaillées relatives aux microprogrammes du serveur sont horodatées à la fin de l'opération de détection ou de mise à jour. Les informations sont écrites à un emplacement persistant du module Onboard Administrator avec un journal du dernier événement de gestion des microprogrammes. Ces informations de microprogramme et ce journal sont également synchronisés avec le module Onboard Administrator en Standby, s'il en existe un.

Gestion de boîtiers

Mise hors tension du boîtier

Deux méthodes permettent de mettre hors tension un boîtier :

- Mettez hors tension le module PDU qui alimente le boîtier.
- Débranchez le ou les câbles d'alimentation du boîtier.

Le module Onboard Administrator ne propose pas de méthode virtuelle pour mettre hors tension un boîtier.

Liaison de boîtiers

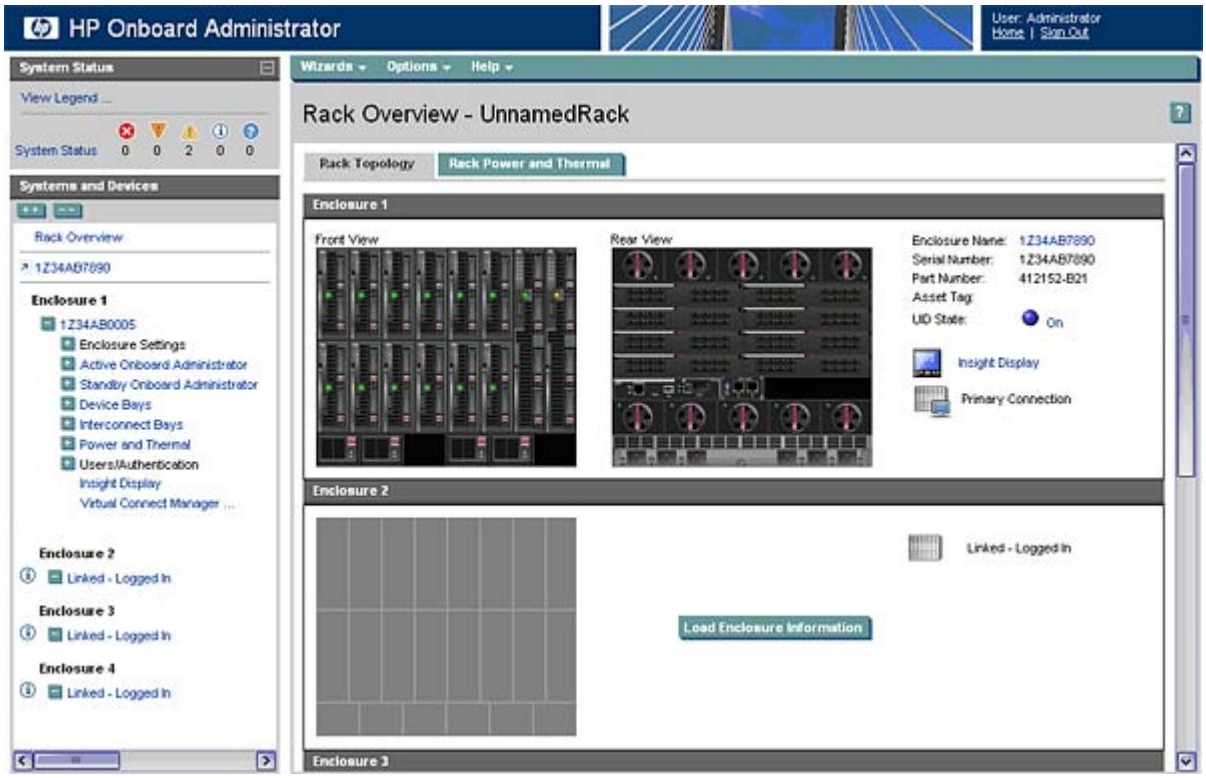
Vous pouvez lier des boîtiers, depuis l'arrière de chacun d'eux. Pour plus d'informations, consultez le Manuel d'installation et de configuration du boîtier HP BladeSystem c7000.

Gestion de plusieurs boîtiers

Dans le menu principal des sections Systems and Devices (Systèmes et périphériques) de l'écran, chaque boîtier est identifié par son nom unique (le nom de boîtier par défaut est le numéro de série du boîtier). Si vous cliquez sur la case bleue qui contient un signe plus (+), la vue du boîtier se développe et permet ainsi d'accéder aux sous-catégories des lames, des ventilateurs, des alimentations, des modules Onboard Administrator et des commutateurs du boîtier.

Pour identifier physiquement le boîtier sur lequel vous travaillez, appuyez sur le bouton UID du module Onboard Administrator. Cette action allume un voyant bleu brillant situé sur le plateau. Pour mettre l'UID hors tension, appuyez de nouveau sur le bouton UID du module Onboard Administrator. L'écran Enclosures (Boîtiers) présente deux sections qui peuvent vous aider à identifier le boîtier auquel vous êtes rattaché (en surbrillance dans l'image ci-dessous).

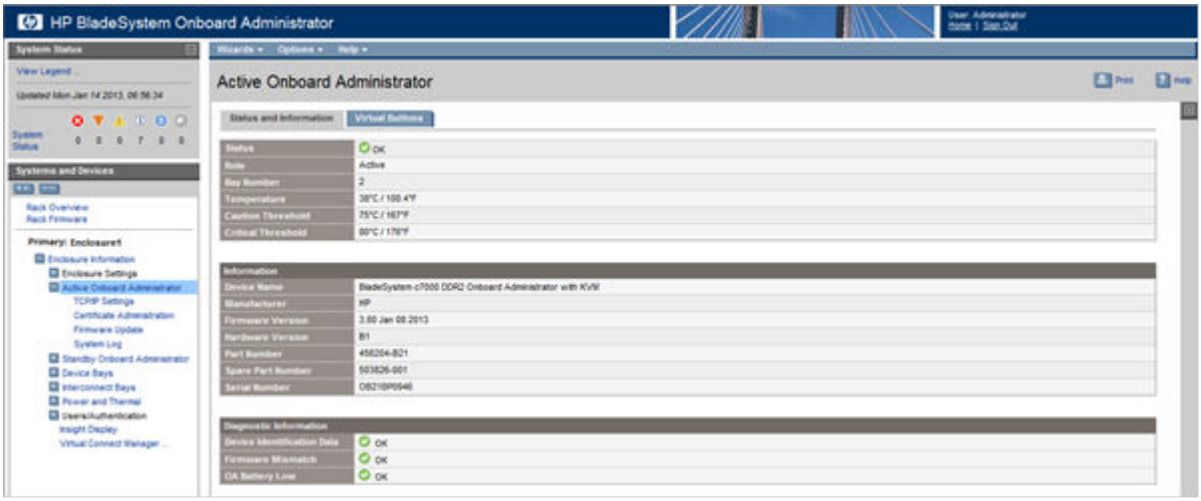
- Sous Rack Overview (Vue d'ensemble du rack), le nom du boîtier auquel vous êtes connecté est affiché.
- Dans la liste de boîtiers, le boîtier auquel vous êtes connecté affiche Primary Connection (Connexion principale).



Module Onboard Administrator actif

Écran Active Onboard Administrator

Dans l'onglet Status and Information (État et informations) de l'écran Active Onboard Administrator (Onboard Administrator actif), trois tableaux présentent des informations détaillées sur votre module Onboard Administrator.



Onglet Status and Information

REMARQUE : L'accès au module OA actif via l'adresse IPv6 d'un lien-local est susceptible de ne pas fonctionner sur certaines configurations système client contenant plusieurs interfaces réseau.

Informations d'état

Rangée	Description
Status (État)	État global du boîtier. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Failed (Échec).
Role (Rôle)	Les valeurs possibles sont Active (Actif) et Standby (Mode Standby).
Bay Number (Numéro de baie)	Numéro de la baie physique dans laquelle le module Onboard Administrator est installé.
Temperature (Température)	Température du module Onboard Administrator exprimée en degrés Celsius et Fahrenheit.
Caution Threshold (Seuil d'avertissement)	La température à laquelle le boîtier signalera un état d'avertissement.
Critical Threshold (Seuil critique)	Température à laquelle le boîtier signalera un état critique.

Informations matérielles

Rangée	Description
Device Name (Nom du périphérique)	Nom descriptif commun du module Onboard Administrator
Manufacturer (Fabricant)	Nom de la société qui a fabriqué le module Onboard Administrator
Firmware Version (Version du microprogramme)	Version de l'image du microprogramme dans le module Onboard Administrator
Hardware Version (Version du matériel)	La version du matériel de boîtier
Part Number (Référence)	Numéro de référence à utiliser pour commander un module Onboard Administrator supplémentaire ou de remplacement

Rangée	Description
Spare Part Number (Numéro de la pièce de rechange)	Numéro de pièce de rechange à utiliser pour commander un module Onboard Administrator supplémentaire ou de remplacement
Serial Number (Numéro de série)	Numéro de série unique du module Onboard Administrator

Informations de diagnostics

Les informations de diagnostics sont recueillies de deux façons : Par interrogation du microcontrôleur de périphérique (résultat d'un état détérioré si une panne s'est produite) ou envoyées par le microcontrôleur du périphérique, sans interrogation, pour signaler une panne.

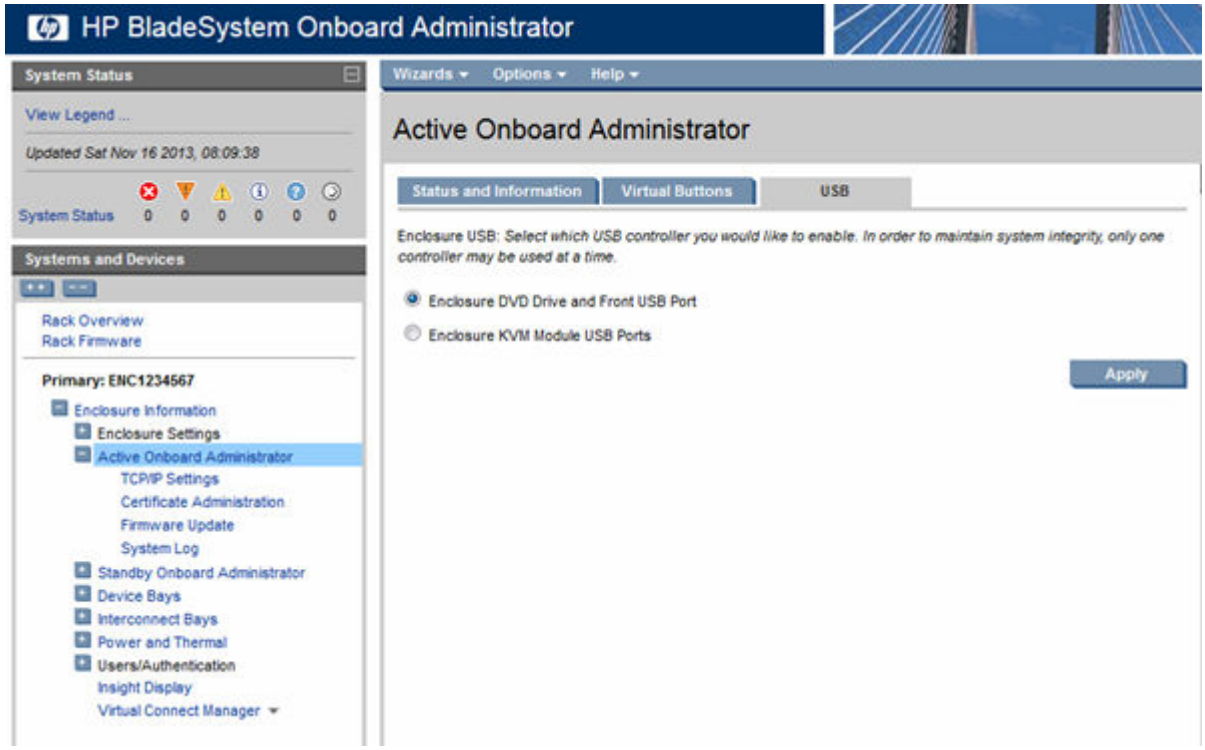
Rangée	Description
Device Identification Data (Données d'identification du périphérique)	Cette ligne contient des informations telles que le nom du modèle, la référence, le numéro de série, ainsi que d'autres informations utilisées pour identifier le périphérique. Ces données sont également appelées données FRU. Une erreur de données d'identification du périphérique s'affiche si les données sont absentes ou illisibles par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Firmware Mismatch (Discordance de microprogramme)	Le module Onboard Administrator doté de la version de microprogramme la plus basse affiche ce champ lorsque deux modules Onboard Administrator sont présents.
Batterie OA	État de la batterie du module Onboard Administrator. Les valeurs possibles sont OK et Error.

Onglet Virtual Buttons du module Onboard Administrator actif

Cliquez sur **Reset** (Réinitialiser) pour réinitialiser le module Onboard Administrator. Un écran de confirmation s'affiche, vous invitant à confirmer que vous souhaitez exécuter l'action et vous indiquant que vous serez déconnecté du module Onboard Administrator. Cliquez sur **OK** pour continuer, ou sur **Cancel** (Annuler) pour quitter sans apporter de modification.

Cliquez sur **Toggle On/Off** (Activé/Désactivé) pour modifier le voyant d'UID du module Onboard Administrator. Ce bouton est utile pour identifier un module Onboard Administrator spécifique en cas de présence de plusieurs.

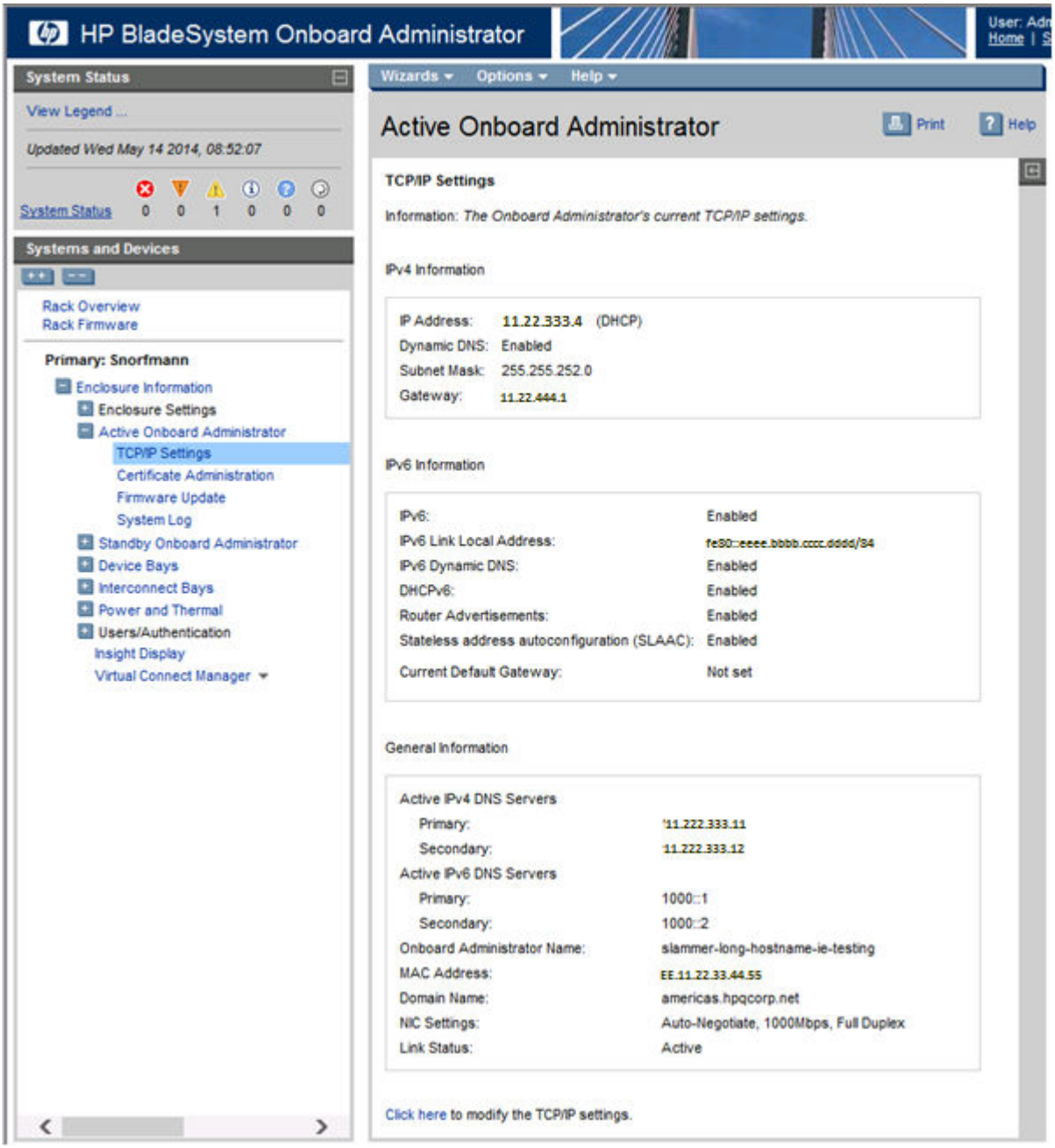
Onglet USB du module Onboard Administrator actif



L'onglet **USB** apparaît uniquement si une version antérieure de la carte c3000 Onboard Administrator (niveau de révision du matériel A0, B0, X1 ou X3) est présent.

Avec ces cartes, vous ne pouvez utiliser qu'un contrôleur USB à la fois. Cet écran vous permet de sélectionner le contrôleur USB à activer : celui pour les ports USB sur le module KVM à l'arrière du boîtier ou celui pour le lecteur DVD et le port USB à l'avant du boîtier. La modification du contrôleur USB actif réinitialise le module Onboard Administrator actif.

Écran TCP/IP Settings du module Onboard Administrator actif



Cet écran affiche les paramètres TCP/IP du boîtier actuel pour le module Onboard Administrator actif :

- Informations IPv4
- Informations IPv6
- Informations générales

Informations IPv4

Paramètre	Description
IP Address (Adresse IP)	L'adresse IPv4 du module Onboard Administrator actif, avec indication du type d'adresse IP affectée (statique ou dynamique).
Dynamic DNS (DNS dynamique)	Indique si le DNS dynamique est activé ou désactivé. Le DNS dynamique met à jour le serveur DNS avec des enregistrements nouveaux ou modifiés pour les adresses IP. Cela permet d'utiliser le même nom d'hôte au fil du temps, bien que l'adresse IP attribuée dynamiquement puisse changer pour le module Onboard Administrator actif.
Subnet Mask (Masque de sous-réseau)	Masque de sous-réseau du module Onboard Administrator actif. Le masque détermine à quel sous-réseau appartient l'adresse IP du module Onboard Administrator actif.
Gateway (Passerelle)	L'adresse de passerelle pour le module Onboard Administrator actif.

Informations IPv6

Paramètre	Description
IPv6	Indique si IPv6 est activé ou désactivé sur le module Onboard Administrator actif
IPv6 Link Local Address (Adresse locale du lien IPv6)	Adresse IPv6 locale du lien du module Onboard Administrator actif. Lorsque IPv6 est activé, une adresse IPv6 locale de lien est configurée automatiquement pour le module Onboard Administrator actif.
IPv6 Static Address 1 (Adresse statique 1 IPv6)	Adresse IPv6 1 de carte réseau externe du module Onboard Administrator.
IPv6 Static Address 2 (Adresse statique 2 IPv6)	Adresse IPv6 2 de carte réseau externe du module Onboard Administrator.
IPv6 Static Address 3 (Adresse statique 3 IPv6)	Adresse IPv6 3 de carte réseau externe du module Onboard Administrator.
IPv6 Dynamic DNS (DNS dynamique IPv6)	Indique si le DNS dynamique est activé ou désactivé. Le DNS dynamique met à jour le serveur DNS avec des enregistrements nouveaux ou modifiés pour les adresses IP. Cela permet d'utiliser le même nom d'hôte au fil du temps, bien que l'adresse IP attribuée dynamiquement puisse changer pour le module Onboard Administrator actif.
DHCPv6	Indique si DHCPv6 est activé ou désactivé sur le module Onboard Administrator actif.
DHCPv6 Address (Adresse DHCPv6)	Adresse DHCPv6 du module Onboard Administrator actif.
Router Advertisements (Annonces de routeur)	Indique si les annonces de routeur sont activées ou désactivées. Les annonces de routeur sont utilisées pour configurer automatiquement les adresses IPv6. Lorsqu'elles sont désactivées, les annonces de routeur sont bloquées, empêchant ainsi la configuration de l'adresse SLAAC de tous les périphériques dans le boîtier.
Stateless address autoconfiguration (SLAAC)	Indique si SLAAC est activé ou désactivé sur le module Onboard Administrator actif. Les annonces de routeur doivent être activées. Consultez la description des annonces de routeur.
Stateless address autoconfiguration (SLAAC) Address (Adresse SLAAC)	Une adresse SLAAC auto-configurée. Le module Onboard Administrator peut se voir attribué plusieurs adresses SLAAC en fonction de son adresse MAC et des informations reçues à partir d'annonces de routeur.

Paramètre	Description
Current Default Gateway (Passerelle par défaut actuelle)	Indique l'adresse IPv6 de la passerelle par défaut actuellement utilisée par le module Onboard Administrator actif. La passerelle par défaut actuelle peut être la passerelle statique par défaut ou une passerelle configurée via des annonces de routeur. Si des annonces de routeur fournissent la configuration de passerelle IPv6, leur configuration de passerelle remplace le paramètre de passerelle IPv6 statique.
Static Default Gateway (Passerelle statique par défaut)	Indique l'adresse IPv6 statique de la passerelle par défaut IPv6. Celle-ci est affichée uniquement si elle est configurée.
Static Route 1 (Route statique 1)	L'adresse du nœud ou du réseau externe que le module Onboard Administrator peut atteindre au travers d'une passerelle de route statique associée.
Gateway (Static Route 1) (Passerelle [Route statique 1])	L'adresse de la passerelle utilisée par le module Onboard Administrator pour accéder à la destination de route statique 1.
Static Route 2 (Route statique 2)	Une deuxième route statique IPv6.
Gateway (Static Route 2) (Passerelle [Route statique 2])	L'adresse de la passerelle utilisée par le module Onboard Administrator pour accéder à la destination de route statique 2.
Static Route 3 (Route statique 3)	Une troisième route statique IPv6.
Gateway (Static Route 3) (Passerelle [Route statique 3])	L'adresse de la passerelle utilisée par le module Onboard Administrator pour accéder à la destination de route statique 3.

Informations générales

Paramètre	Description
Active IPv4 DNS Servers (Serveurs DNS IPv4 actifs)	Répertorie les serveurs DNS IPv4 configurés qui sont actifs sur le module Administrator Onboard actif.*
Primary (Principal)	Adresse IP du premier serveur DNS IPv4 utilisé par le module Onboard Administrator actif. Si non configuré, `Not set` est affiché.
Secondary (Secondaire)	Adresse IP du second serveur DNS IPv4 utilisé par le module Onboard Administrator actif. Si non configuré, `Not set` est affiché.
Active IPv6 DNS Servers (Serveurs DNS IPv6 actifs)	Répertorie les serveurs DNS IPv6 configurés qui sont actifs sur le module Administrator Onboard actif.*
Primary (Principal)	Adresse IP du premier serveur DNS IPv6 utilisé par le module Onboard Administrator actif. Si non configuré, `Not set` est affiché.
Secondary (Secondaire)	Adresse IP du second serveur DNS IPv6 utilisé par le module Onboard Administrator actif. Si non configuré, `Not set` est affiché.
Tertiary (Tertiaire)	Adresse IP du troisième serveur DNS IPv6 utilisé par le module Onboard Administrator actif. Si non configurés, ce paramètre et l'adresse ne sont pas affichés.
Quaternary (Quaternaire)	Adresse IP du quatrième serveur DNS utilisé par le module Onboard Administrator actif. Si non configurés, ce paramètre et l'adresse ne sont pas affichés.
Onboard Administrator Name (Nom du module Onboard Administrator)	Nom (nom d'hôte DNS) utilisé pour le module Onboard Administrator actif.

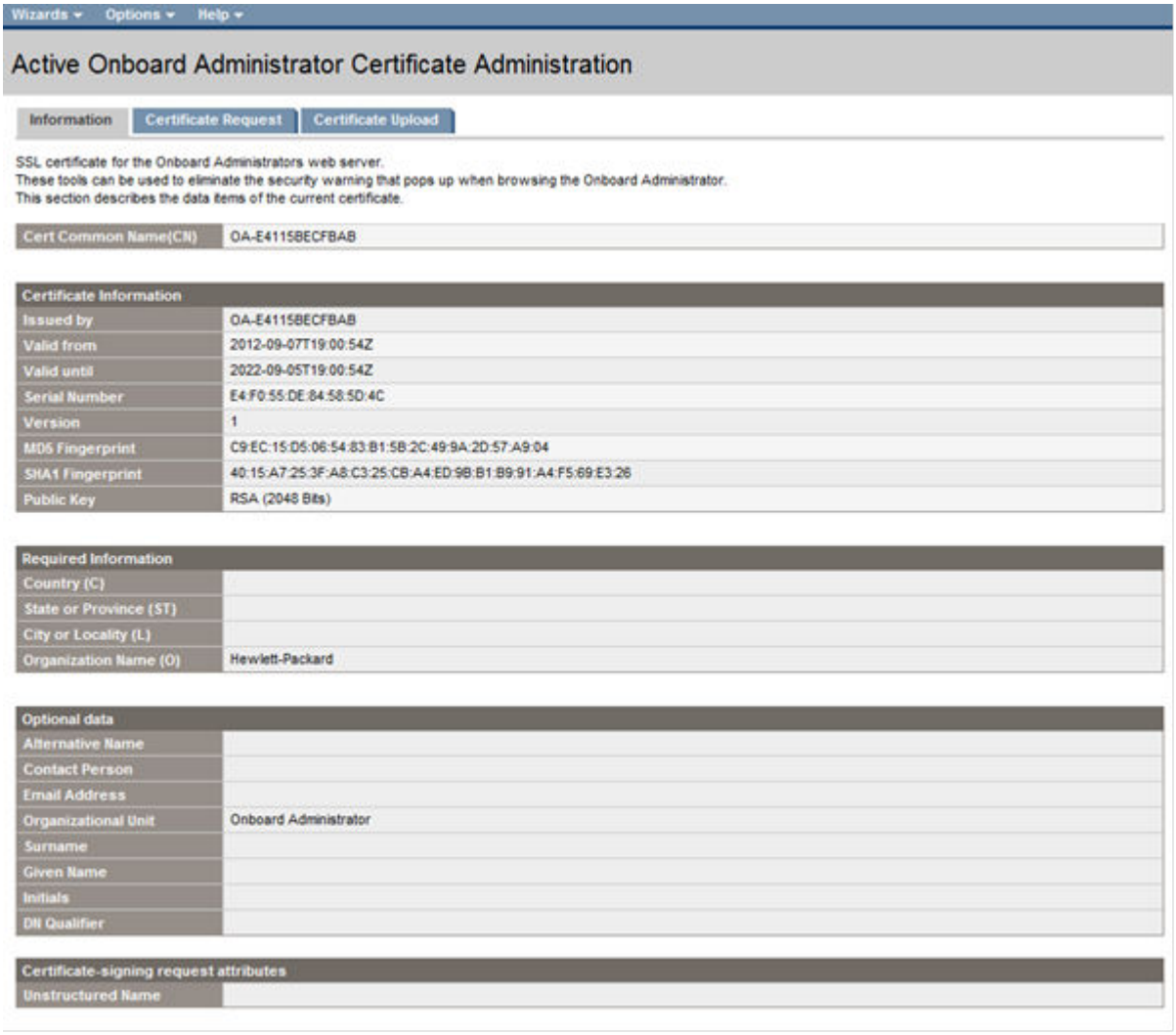
Paramètre	Description
VLAN ID (Name) (ID VLAN [Nom])	Numéro unique qui identifie le réseau VLAN. Affiché uniquement si le mode VLAN est activé.
MAC Address (Adresse MAC)	Adresse MAC du module Onboard Administrator actif.
Domain Name (Nom de domaine)	Nom du domaine du module Onboard Administrator actif.
NIC Settings (Paramètres de carte réseau)	Les paramètres de carte réseau pour le module Onboard Administrator actif, tels que négociation automatique, mode duplex et vitesse.
Link Status (État de liaison)	Indique si la carte réseau est activement connectée au réseau.

* L'ordre dans lequel le module Onboard Administrator utilise des serveurs DNS est décrite dans l'onglet IPv4 Settings (Onglet IPv4 Settings à la page 126) et l'onglet IPv6 Settings (Onglet IPv6 Settings à la page 129).

Pour modifier les paramètres TCP/IP, sélectionnez **Click here** (Cliquer ici).

Pour plus d'informations sur les paramètres TCP/IP que vous pouvez modifier, consultez l'onglet Enclosure TCP/IP IPv4 Settings (Onglet IPv4 Settings à la page 126) et l'onglet IPv6 Settings (Onglet IPv6 Settings à la page 129).

Onglet d'informations d'administration de certificat



Onglet Informations

Cet écran affiche des informations détaillées concernant le certificat SSL actuellement utilisé par le module Onboard Administrator. Un certificat SSL est utilisé pour certifier l'identité du module Onboard Administrator et est requis par le serveur HTTP sous-jacent pour établir un canal de communications sécurisé (crypté) avec le navigateur Web du client.

Au démarrage initial, le module Onboard Administrator génère un certificat SSL auto-signé par défaut valide pour 10 ans, et le certificat est émis au nom du module Onboard Administrator. Dans la mesure où ce certificat par défaut est auto-signé, le champ « Issued by » (Émis par) est également défini sur le même nom.

Informations d'état

Rangée	Description
Cert Common Name	Nom commun de l'objet du certificat.

Informations sur le certificat

Rangée	Description
Issued by (Émis par)	Autorité de certification qui a émis le certificat
Valid from (Valide à partir de)	Date à partir de laquelle le certificat est valide
Valid until (Valide jusqu'à)	Date à laquelle le certificat expire
Serial Number (Numéro de série)	Numéro de série attribué au certificat par l'autorité de certification
Version	Numéro de version du certificat actuel
MD5 Fingerprint (Empreinte MD5)	Ce champ est une validation d'authenticité et est incorporé dans le certificat
SHA1 Fingerprint (Empreinte SHA1)	Ce champ est une validation d'authenticité et est incorporé dans le certificat
Public Key (Clé publique)	Nom de la clé publique.

Informations requises

Rangée	Description
Country (C) (Pays)	Code de pays à deux caractères qui identifie le pays dans lequel le module Onboard Administrator est situé.
State or Province (ST) (État ou province)	État ou province dans lequel/laquelle est installé le module Onboard Administrator.
City or Locality (L) (Ville ou localité)	Ville ou localité dans laquelle est installé le module Onboard Administrator.
Organization Name (O) (Nom d'organisation)	Société qui possède ce module Onboard Administrator.

Données facultatives

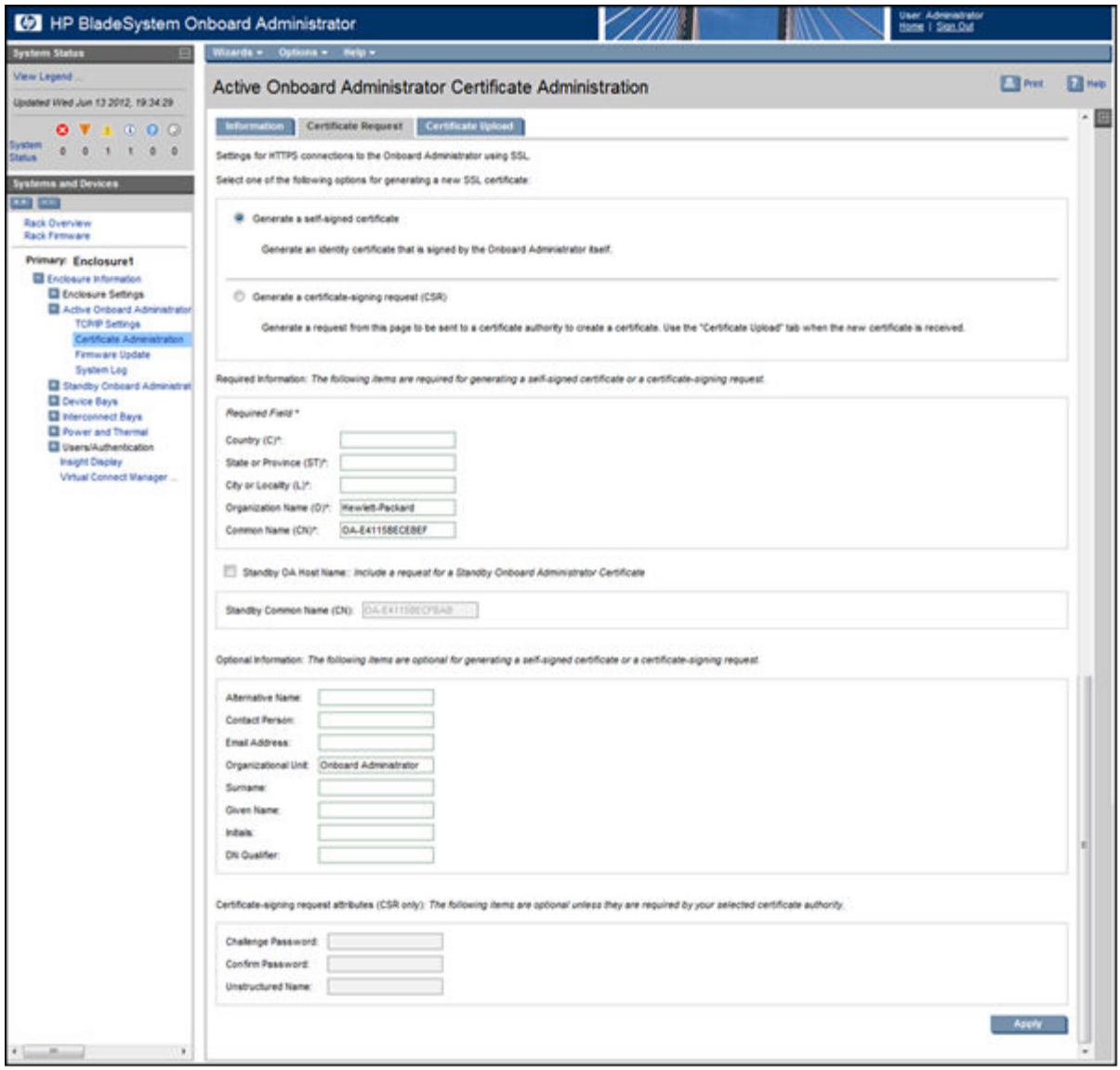
Rangée	Description
Alternative Name (Nom secondaire)	Autre nom du module Onboard Administrator.
Contact Person (Contact)	Personne responsable du module Onboard Administrator.
Email Address (Adresse électronique)	Adresse électronique de la personne responsable du module Onboard Administrator.
Organizational Unit (Unité organisationnelle)	Unité, au sein de l'entreprise ou de l'organisation, qui possède le module Onboard Administrator.
Surname (Nom)	Nom de famille de la personne responsable du module Onboard Administrator.
Given Name (Prénom)	Prénom de la personne responsable du module Onboard Administrator.
Initials (Initiales)	Initiales de la personne responsable du module Onboard Administrator.
DN Qualifier (Qualificatif de nom distinctif)	Qualificatif de nom distinctif du module Onboard Administrator.

Attributs de demande de signature de certificat

Rangée	Description
Unstructured Name (Nom non structuré)	Destiné à des informations supplémentaires.

Onglet Certificate Request

L'onglet Certificate Request (Demande de certificat) permet d'entrer les informations requises pour générer un certificat auto-signé ou une demande de signature de certificat normalisé vers une autorité de certificats.



Informations requises

Champ	Valeurs possibles	Description
Country (C) (Pays)	Doit comporter 1 ou 2 caractères. Les caractères autorisés sont tous les caractères alphanumériques, les espaces et les signes de ponctuation suivants : ' ( ) + , - . / : = ?	Code de pays valide qui identifie le pays dans lequel le module Onboard Administrator est situé.
State or Province (ST) (État ou province)	Doit comporter entre 1 et 30 caractères.	État ou province dans lequel/laquelle est installé le module Onboard Administrator.
City or Locality (L) (Ville ou localité)	Doit comporter entre 1 et 50 caractères.	Ville ou localité dans laquelle est installé le module Onboard Administrator.
Organization Name (O) (Nom d'organisation)	Doit comporter entre 1 et 60 caractères.	Organisation qui possède ce module Onboard Administrator. Lorsque cette information est utilisée pour générer une requête de signature de certificat, l'autorité délivrant le certificat peut vérifier que l'organisation demandeuse est effectivement en droit de se déclarer propriétaire de ladite organisation ou entreprise.
Common Name (CN) (Nom commun)	Doit comporter entre 1 et 60 caractères. Pour éviter des alertes de sécurité, la valeur de ce champ doit correspondre exactement au nom d'hôte tel qu'il est connu par le navigateur Web. Le navigateur Web compare le nom d'hôte apparaissant dans l'adresse Web résolue avec celui spécifié dans le certificat. Par exemple, si l'adresse Web dans le champ d'adresse est https://oa-001635.xyz.com, la valeur doit être oa-001635.xyz.com.	Nom du module Onboard Administrator indiqué dans le champ d'adresse Web. Cet attribut de certificat est plus connu sous le nom de nom commun.

Sélectionnez **Standby OA Host Name** pour inclure une demande de certificat de module Onboard Administrator en mode Standby. Entrez les informations dans le champ **Standby Common Name (CN)**, avec une longueur comprise entre 1 et 60 caractères. Cette sélection s'affiche uniquement si le boîtier contient un module Onboard Administrator en mode Standby.

Informations facultatives

Champ	Valeurs possibles	Description
Alternative Name (Nom secondaire)	Doit comporter entre 0 et 511 caractères.	Autre nom du module Onboard Administrator. Le nom est utilisé pour la création de l'attribut d'extension du nom d'objet secondaire X509v3. Le champ doit soit être vide soit contenir une liste de paires mot-clé-valeur séparées par des virgules. Les entrées mot-clé-valeur valides incluent IP:<adresse_ip> et DNS:<nom_domaine>.
Contact Person (Contact)	Doit comporter entre 0 et 60 caractères.	Personne responsable du module Onboard Administrator.

Champ	Valeurs possibles	Description
Email Address (Adresse électronique)	Doit comporter entre 0 et 60 caractères.	Adresse e-mail de la personne responsable du module Onboard Administrator.
Organizational Unit (Unité organisationnelle)	Doit comporter entre 0 et 60 caractères.	Unité, au sein de l'entreprise ou de l'organisation, qui possède le module Onboard Administrator.
Surname (Nom)	Doit comporter entre 0 et 60 caractères.	Nom de famille de la personne responsable du module Onboard Administrator.
Given Name (Prénom)	Doit comporter entre 0 et 60 caractères.	Prénom de la personne responsable du module Onboard Administrator.
Initials (Initiales)	Doit comporter entre 0 et 20 caractères.	Initiales de la personne responsable du module Onboard Administrator.
DN Qualifier (Qualificatif de nom distinctif)	Doit comporter entre 0 et 60 caractères. Les caractères autorisés sont tous les caractères alphanumériques, les espaces et les signes de ponctuation suivants : ' ( ) + , - . / : = ?	Qualificatif de nom distinctif du module Onboard Administrator.

Attributs de demande de signature de certificat

Champ	Valeurs possibles	Description
Challenge Password (Mot de passe)	Longueur comprise entre 0 et 30 caractères	Mot de passe de demande de signature du certificat
Confirm Password (Confirmer le mot de passe)	Longueur comprise entre 0 et 30 caractères	Confirmation du mot de passe
Unstructured Name (Nom non structuré)	Longueur comprise entre 0 et 60 caractères	Destiné à des informations supplémentaires comme, par exemple, un nom non structuré qui est attribué au module Onboard Administrator

Pour générer un certificat auto-signé ou une demande de signature de certificat normalisé, cliquez sur **Apply** (Appliquer).

Demande de signature de certificat normalisé

Cet écran affiche une demande de signature de certificat normalisé générée par le module Onboard Administrator. Le contenu de la demande dans la zone de texte peut être envoyé à une autorité de certification de votre choix pour signature. Une fois signé et renvoyé par l'autorité de certification, le certificat peut être téléchargé sous l'onglet Certificate Upload (Téléchargement de certificat).

Si une adresse IP statique est configurée pour le module Onboard Administrator lorsque cette demande de certificat est générée, cette dernière sera émise vers l'adresse IP statique. Sinon, elle est émise vers le nom DNS dynamique du module Onboard Administrator. Par défaut, le certificat demande une durée de validité de 10 ans (cette valeur n'est actuellement pas configurable).

Lorsque vous soumettez la demande à l'autorité de certification, assurez-vous :

1. D'utiliser l'URL du module Onboard Administrator pour le serveur.
2. De demander que le certificat soit généré au format RAW.
3. D'inclure les lignes Begin (Début) et End (Fin) du certificat.

Onglet Certificate Upload

Pour charger des certificats à utiliser dans le module HP BladeSystem Onboard Administrator, l'utilisateur doit être connecté à l'aide du compte administrateur.

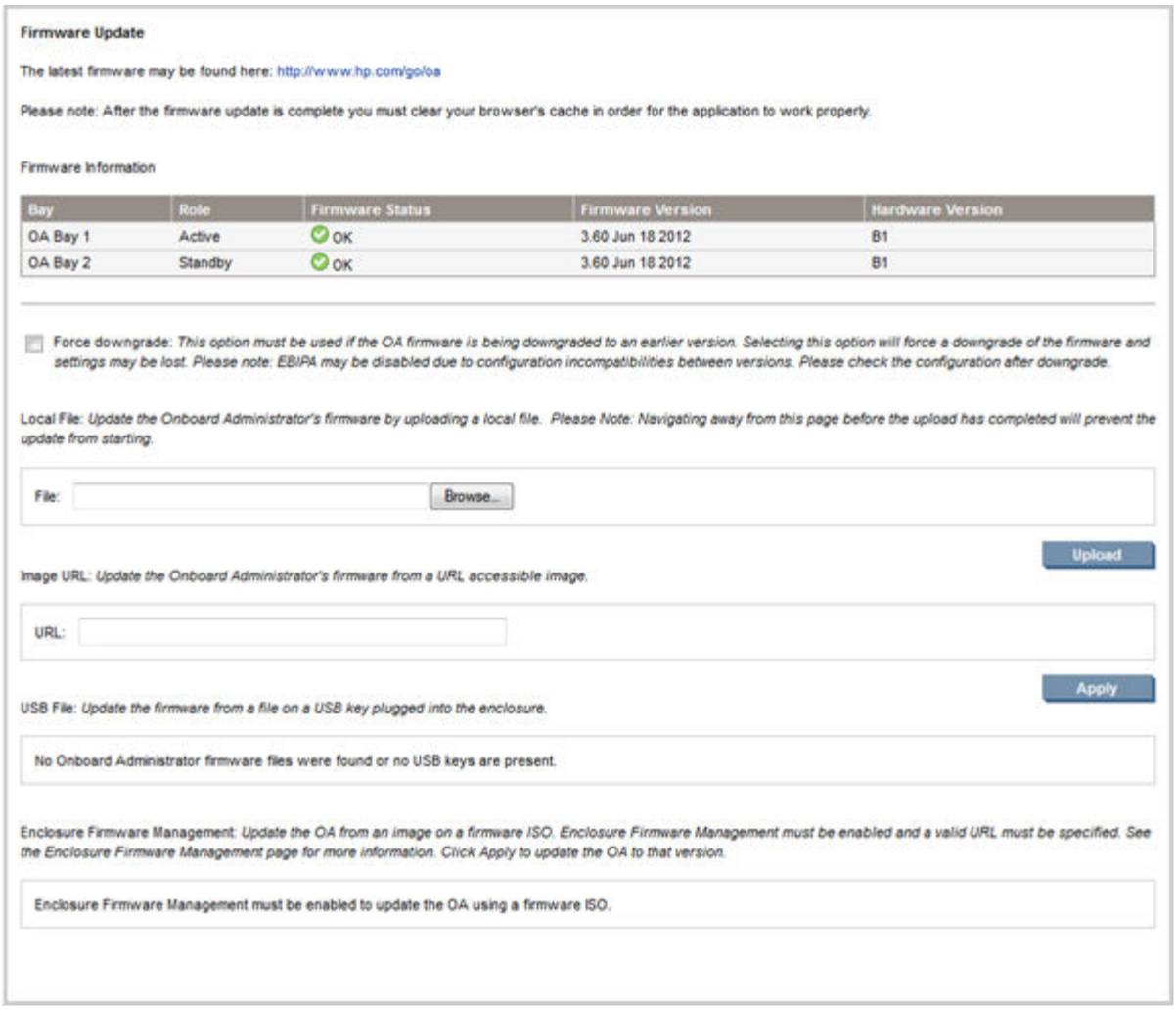
Vous pouvez utiliser deux méthodes pour télécharger des certificats en vue de les utiliser dans le module HP BladeSystem Onboard Administrator :

- Collez le contenu du certificat dans la zone de texte et sélectionnez **Upload** (Télécharger).
- Collez l'URL complète du certificat dans le champ URL et sélectionnez **Apply** (Appliquer).

Le certificat à télécharger doit provenir d'une demande de certificat envoyée et signée par une autorité de certification pour ce module Onboard Administrator donné. Sinon, le certificat ne correspond pas aux clés privées utilisées pour générer la demande de certificat, et le certificat est rejeté. En outre, si le domaine du module Onboard Administrator a été détruit ou réimporté, vous devrez à nouveau répéter la procédure de génération d'une demande de certificat. Il sera signé par une autorité de certification car les clés privées sont détruites et recréées ainsi que le domaine du module Onboard Administrator.

Si le nouveau certificat est accepté et installé avec succès par le module Onboard Administrator, vous êtes automatiquement déconnecté. Le serveur HTTP doit être redémarré pour que le nouveau certificat prenne effet.

Mise à jour du microprogramme


Firmware Update
The latest firmware may be found here: http://www.hp.com/go/oa
Please note: After the firmware update is complete you must clear your browser's cache in order for the application to work properly.
Firmware Information
Bay
Role
Firmware Status
Firmware Version
Hardware Version
OA Bay 1
Active
OK
3.60 Jun 18 2012
B1
OA Bay 2
Standby
OK
3.60 Jun 18 2012
B1
Force downgrade: This option must be used if the OA firmware is being downgraded to an earlier version. Selecting this option will force a downgrade of the firmware and settings may be lost. Please note: EBIPA may be disabled due to configuration incompatibilities between versions. Please check the configuration after downgrade.
Local File: Update the Onboard Administrator's firmware by uploading a local file. Please Note: Navigating away from this page before the upload has completed will prevent the update from starting.
File:
Browse...
Upload
Image URL: Update the Onboard Administrator's firmware from a URL accessible image.
URL:
Apply
USB File: Update the firmware from a file on a USB key plugged into the enclosure.
No Onboard Administrator firmware files were found or no USB keys are present.
Enclosure Firmware Management: Update the OA from an image on a firmware ISO. Enclosure Firmware Management must be enabled and a valid URL must be specified. See the Enclosure Firmware Management page for more information. Click Apply to update the OA to that version.
Enclosure Firmware Management must be enabled to update the OA using a firmware ISO.

ATTENTION : Lorsqu'une mise à niveau du microprogramme est en cours, ne déconnectez pas ou n'arrêtez pas les modules Onboard Administrator. Cela peut rendre la lame de serveur ou le module Onboard Administrator inutilisable.

La version actuelle du microprogramme installé sur le module Onboard Administrator, actif et Standby, apparaît sur cet écran. La version actuelle du matériel du module Onboard Administrator apparaît sur cet écran.

Pour obtenir la version la plus récente du microprogramme pour votre module Onboard Administrator, visitez le site Web HP Onboard Administrator (http://www.hp.com/go/oa). Pour obtenir des informations détaillées sur la mise à niveau de modules Onboard Administrator dans les boîtiers HP BladeSystem c3000 et c7000, consultez la section « Mise à niveau de modules Onboard Administrator dans un boîtier HP BladeSystem » (Mise à niveau de modules Onboard Administrator dans un boîtier HP BladeSystem à la page 224).

Synchronisation du microprogramme

Pour synchroniser le microprogramme sur les modules Onboard Administrator actif et Standby sur la même version de microprogramme, cliquez sur **Synchronize Firmware** (Synchroniser le microprogramme). Une image du microprogramme est créée à partir du contenu flash du module Onboard Administrator ayant la version de microprogramme la plus récente et est programmée sur le

module Onboard Administrator doté de la version de microprogramme la plus ancienne. Le module Onboard Administrator mis à niveau redémarre une fois le microprogramme programmé.

Pour utiliser la fonction Synchronize Firmware :

- Les deux modules Onboard Administrator doivent exécuter la version 2.10 ou ultérieure du microprogramme.
- Si VLAN est activé sur le module Onboard Administrator actif, le module Onboard Administrator en Standby doit être doté d'un microprogramme compatible avec la fonction VLAN. Si le module Onboard Administrator en Standby comporte une version de microprogramme plus ancienne qui ne prend pas en charge VLAN, vous devez retirer le module Onboard Administrator en Standby et mettre à jour le microprogramme à une version compatible à partir d'un boîtier différent.

Rétrogradation de microprogramme

Force Downgrade (Forcer la rétrogradation) : utilisez cette option pour forcer une dégradation du module Onboard Administrator à une version antérieure. La sélection de cette option provoque la dégradation du microprogramme ; les paramètres actuels qui sont inapplicables à la version antérieure peuvent être perdus. Lorsque le module Onboard Administrator est en mode VC et a l'IPv6 activé, Virtual Connect Manager peut spécifier une version minimum du microprogramme attendue pour le module Onboard Administrator. Lorsque cette situation se produit, la désactivation de la communication IPv6 du module Onboard Administrator avant la tentative de rétrogradation permet à VC d'interagir avec des versions antérieures du module Onboard Administrator.

REMARQUE : Cette fonction est désactivée en mode FIPS ON/DEBUG.

Mettre à jour le microprogramme

ATTENTION : En mode FIPS ON/DEBUG, une mise à niveau vers la version actuelle du module Onboard Administrator à partir d'une version antérieure à 4.40 conserve les 21 premiers comptes utilisateur locaux qui ont été créés, y compris les comptes réservés tels que les utilisateurs Administrateur et Virtual Connect. Les autres utilisateurs sont supprimés.

REMARQUE : La mise à jour du microprogramme OA à partir d'une version OA antérieure à 3.50 vers OA 4.50 ou version ultérieure nécessite tout d'abord une mise à jour intermédiaire vers OA 3.50. Si vous mettez à jour le microprogramme OA à partir de l'écran Firmware Update, vous devez procéder manuellement à cette mise à jour intermédiaire avant d'effectuer la mise à jour vers OA 4.50 ou version ultérieure. Le microprogramme OA 3.50 intermédiaire est téléchargeable à partir du site Web HP Onboard Administrator (http://h20564.www2.hp.com/hpsc/swd/public/detail?swItemId=MTX_00b278b5e9194e7ab0ab362d55).

La mise à jour intermédiaire manuelle n'est pas nécessaire en cas de mise à jour du microprogramme OA à partir d'une image ISO FW ou lors de l'utilisation de la fonction Synchronize Firmware à partir de l'écran Active Onboard Administrator Firmware Update

Local File (Fichier local) : pour mettre à jour le microprogramme sur le module Onboard Administrator actif à partir d'un fichier local, naviguez vers le fichier image du microprogramme ou entrez le chemin du fichier image du microprogramme dans la zone de texte. Le nombre maximum de caractères dans le chemin du fichier est 256. Cliquez sur **Upload** (Charger).

Image URL (URL de l'image) : pour mettre à jour le microprogramme sur le module Onboard Administrator actif à partir d'un fichier situé sur un serveur Web :

- Entrez un chemin http:// vers le fichier de l'image du microprogramme. Les protocoles pris en charge sont HTTP, FTP et TFTP. L'URL respecte le format suivant : `protocole://hôte/chemin/nom_fichier`. La syntaxe d'URL pour les adresses IPv6 est :

  `protocole://[adresse_ipv6]/chemin/fichier`

La longueur maximale de l'URL est de 511 caractères. Si votre serveur FTP ne prend pas en charge les connexions anonymes, vous pouvez spécifier un nom d'utilisateur et un mot de passe dans l'URL au format : `ftp://nom_utilisateur:mot_passe@hôte/chemin/nom_fichier`

REMARQUE : Lorsque vous utilisez le protocole FTP, spécifiez le chemin de l'URL de l'image dans ce format, en spécifiant une double barre oblique (//) avant la partie host/path/filename de l'URL : ftp://user:password@//host/path/filename.

REMARQUE : En raison d'un changement de comportement dans Onboard Administrator v4.11, si vous spécifiez une simple barre oblique (/) au lieu de deux barres obliques, certains serveurs FTP vont chercher le fichier image en utilisant votre répertoire de base comme le chemin d'accès racine relatif (/home/user/path/filename). Spécifier les doubles barres obliques recommandées garantit que le serveur FTP utilise le chemin absolu (/path/filename) pour rechercher l'image.

- Entrez l'URL, puis cliquez sur **Apply** (Appliquer).
- Lorsque vous cliquez sur **Upload** (Charger) ou **Apply** (Appliquer), une fenêtre s'affiche pour indiquer l'avancement du téléchargement du microprogramme. Une fois le téléchargement terminé, vous êtes déconnecté du module Onboard Administrator et vous devez vous connecter à nouveau.

USB File (Fichier USB) : pour mettre à jour le microprogramme sur le module Onboard Administrator actif à partir d'une image située sur une clé USB, sélectionnez un fichier à partir du menu, puis cliquez sur **Apply** (Appliquer). Ce champ apparaît uniquement lorsqu'une clé USB est détectée sur le port USB du module Onboard Administrator actif et que des images du microprogramme sont présentes sur la clé USB. La taille maximale de fichier prise en charge pour les clés USB formatées avec FAT32 est de 4 Go. Pour les images SPP supérieures à 4 Go, utilisez une clé USB de format ext2.

Si vous avez lancé la mise à jour du microprogramme, un compteur s'affiche alors que les autres utilisateurs reçoivent une boîte de dialogue qui les informent que le boîtier est mis hors tension et redémarre. Une fois le boîtier redémarré, vous devez à nouveau vous connecter.

Si deux boîtiers sont reliés, le processus de mise à jour du microprogramme fait clignoter le module Onboard Administrator en Standby, puis le module Onboard Administrator principal. Si une connexion ne peut pas être établie immédiatement après une mise à jour du microprogramme, patientez pendant 30 secondes pour permettre au boîtier d'être de nouveau disponible sur le réseau.

Enclosure Firmware Management

Vous pouvez mettre à jour le module Onboard Administrator à partir d'une image sur une image de microprogramme. L'utilitaire Enclosure Firmware Management doit être activé, et une URL valide doit être spécifiée dans les paramètres Enclosure Firmware Management. Pour plus d'informations, consultez la section « Enclosure Firmware Management » (Enclosure Firmware Management à la page 195).

Pour mettre à jour le module Onboard Administrator, cliquez sur **Apply** (Appliquer).

Installation d'une version antérieure

Pour installer une version antérieure du microprogramme, cochez la case **Force downgrade** (Forcer la rétrogradation) dans la section Firmware Information (Informations du microprogramme) de l'écran. Sélectionnez le fichier du microprogramme en le recherchant localement ou en repérant une URL à l'aide des zones de saisie. Si vous abaissez le microprogramme Onboard Administrator à la version 2.31 ou antérieure, vous perdrez tous les groupes d'annuaires au-delà des cinq premiers groupes. Les versions Onboard Administrator ultérieures à la version 2.31 prennent en charge

30 groupes alors que les versions antérieures ne prennent en charge que cinq groupes. Après les cinq premiers groupes, vous verrouillerez les utilisateurs d'annuaire supplémentaires.

Pour réaliser une rétrogradation vers une version précédente avec IPv6 activé, VC nécessite une version minimum du microprogramme du module Onboard Administrator. Pour réaliser la rétrogradation, désactivez IPv6 et réessayez.

Mise à niveau de modules Onboard Administrator dans un boîtier HP BladeSystem

1. Insérez le module de mise à niveau OA dans le boîtier.

   Pour un boîtier c7000 contenant deux modules OA, remplacez le module OA en Standby d'origine par le module de mise à niveau OA.

   Pour un boîtier c7000 contenant un module OA unique, insérez le module de mise à niveau OA dans l'emplacement e module OA vide.

   Pour un boîtier c3000 contenant deux modules OA, assurez-vous que le module OA à remplacer est en mode Standby. Remplacez le module OA en mode Standby par le module de mise à niveau OA.

2. Mettez à jour le microprogramme du module OA actif avec la même version de microprogramme que celle en cours d'exécution sur le module OA actif. Pour cette étape, effectuez la mise à jour du microprogramme à partir de l'écran LCD du boîtier avec une clé USB au format FAT32 contenant le fichier de bin du microprogramme OA et branchée sur le module OA actif (voir l'exemple de menu ci-après). Cela permet de s'assurer que le module de mise à niveau OA exécute la même version de microprogramme. Cela aboutit également à une synchronisation de la configuration du boîtier avec le module de mise à niveau OA.

3. Pour un boîtier c7000 contenant deux modules OA, assurez-vous que le module OA d'origine restant est en mode Standby. Retirez le module OA d'origine restant et insérez un second module de mise à niveau OA. Si le boîtier ne contient qu'un module OA, passez à l'étape suivante.

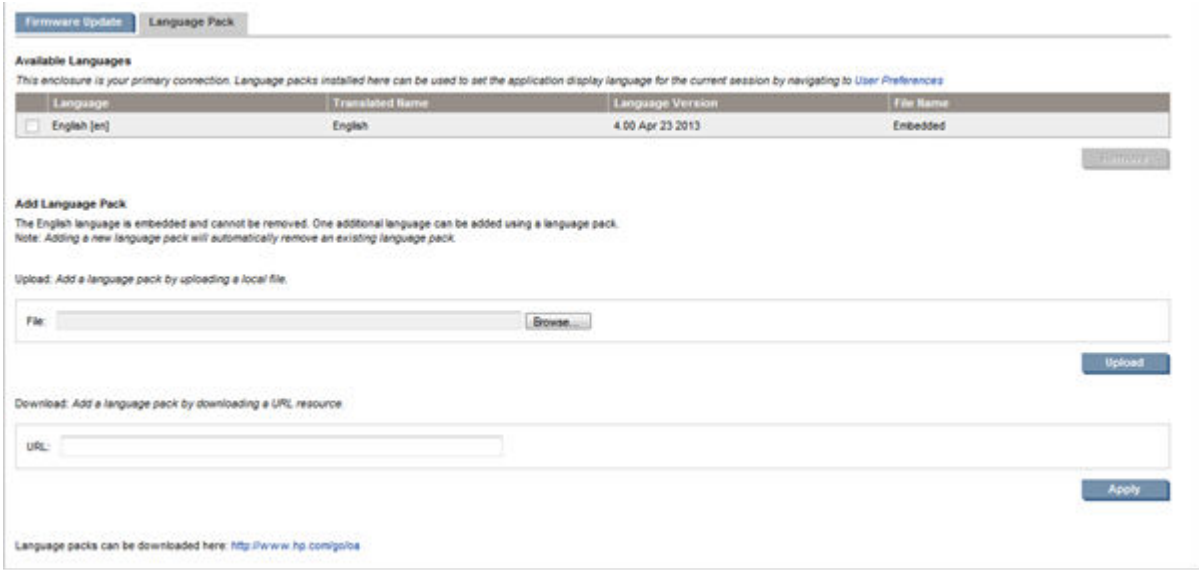
   a. Assurez-vous que le second module de mise à niveau OA a été automatiquement synchronisé avec l'autre module de mise à niveau OA. Pour ce faire, comparez les versions

de microprogramme OA de ce boîtier à partir de l'écran Rack Firmware (Écran Rack Firmware à la page 108).

b. Si les versions de microprogramme ne correspondent pas, mettez à jour le microprogramme du module OA actif. Cela permet de synchroniser la configuration du boîtier avec le module OA actif.

4. Pour un boîtier c7000 contenant un seul module OA, retirez le module OA d'origine après avoir effectué les étapes 1 et 2. Le processus de mise à niveau du boîtier est terminé.

Onglet Language Pack

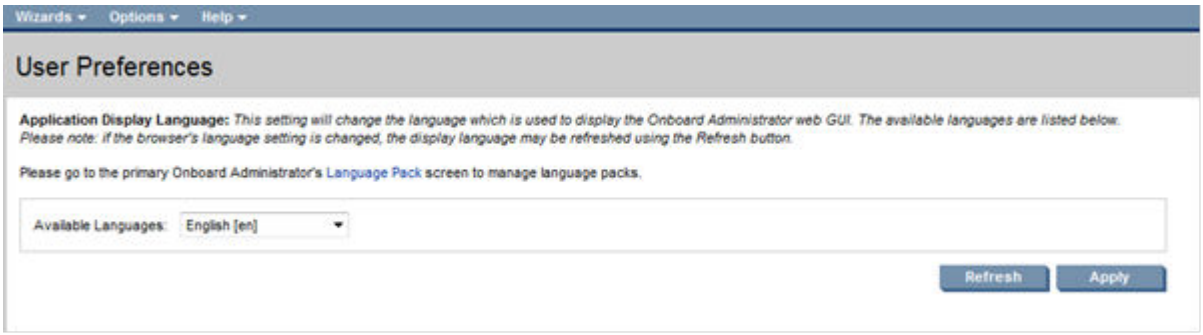

Firmware Update
Language Pack
Available Languages
This enclosure is your primary connection. Language packs installed here can be used to set the application display language for the current session by navigating to User Preferences
Language
Translated Name
Language Version
File Name
English [en]
English
4.00 Apr 23 2013
Embedded
Add Language Pack
The English language is embedded and cannot be removed. One additional language can be added using a language pack.
Note: Adding a new language pack will automatically remove an existing language pack.
Upload: Add a language pack by uploading a local file.
File:
Browse...
Upload
Download: Add a language pack by downloading a URL resource.
URL:
Apply
Language packs can be downloaded here: http://www.hp.com/go/oa

Une liste de packs de langues apparaît sur cet écran. L'anglais est intégré et ne peut pas être supprimé. Seule une langue supplémentaire peut être ajoutée à l'aide d'un pack de langues. L'ajout d'un nouveau pack de langues supprime automatiquement un pack de langues existant. Pour supprimer un pack de langues existant, cochez la case et cliquez sur **Delete** (Supprimer).

Pour ajouter un pack de langues, vous avez deux options :

- **Upload** (Charger) : pour ajouter un pack de langues à partir d'un fichier local, naviguez vers le fichier du pack de langues ou saisissez le chemin du fichier du pack de langues dans la zone de texte. Le nombre maximum de caractères dans le chemin du fichier est 256. Cliquez sur **Upload** (Charger).

- **Download** (Télécharger) : pour ajouter un pack de langues à partir d'un fichier situé sur un serveur Web, saisissez un chemin http:// vers le fichier d'image du microprogramme. Le nombre maximum de caractères dans le chemin du fichier est 255. Les protocoles pris en charge sont HTTP, FTP et TFTP. L'URL respecte le format suivant : protocole://hôte/chemin/nom_fichier. Saisissez l'URL, puis cliquez sur **Apply** (Appliquer). Après avoir cliqué sur Upload (Charger) ou Apply (Appliquer), une fenêtre affiche la progression du téléchargement du microprogramme. Lorsque le téléchargement est terminé, une fenêtre contextuelle affiche le pack de langues comme ajouté.


Wizards
Options
Help
User Preferences
Application Display Language: This setting will change the language which is used to display the Onboard Administrator web GUI. The available languages are listed below. Please note: if the browser's language setting is changed, the display language may be refreshed using the Refresh button.
Please go to the primary Onboard Administrator's Language Pack screen to manage language packs.
Available Languages:
English [en]
Refresh
Apply

Après avoir installé un pack de langues, vous pouvez afficher la langue sur l'interface Onboard Administrator à l'aide de l'option de préférence de langue de votre navigateur actuel (de préférence) ou des options User Preferences du module Onboard Administrator :

- Pour utiliser les paramètres de votre navigateur pour les préférences de langue, ajoutez la langue en haut de liste des langues préférées du navigateur, puis utilisez l'écran User Preferences (Préférences de l'utilisateur à la page 55) du module Onboard Administrator pour sélectionner « Use browser settings » (Utiliser paramètres du navigateur). Cette méthode est recommandée car le paramètre s'applique à toutes les sessions d'interface utilisateur Onboard Administrator ultérieures qui utilisent ce navigateur et pour les sessions avec d'autres modules Onboard Administrator, à condition que la même langue est installée sur les autres interfaces utilisateur Onboard Administrator et que leur paramètre User Preferences correspond à la configuration « Use browser settings » par défaut.
- Pour utiliser l'écran User Preferences (Préférences de l'utilisateur à la page 55) du module Onboard Administrator pour afficher une langue spécifique, sélectionnez la langue dans la liste des langues disponibles et cliquez sur **Apply** (Appliquer). Ce paramètre remplace le paramètre actuel de préférence de langue du navigateur et est conservé avec les sessions d'interface utilisateur se connectant au même module Onboard Administrator. Toutefois, le paramètre ne s'applique pas pour les sessions d'interface utilisateur avec d'autres modules Onboard Administrator. (Le paramètre repose sur un cookie qui est valide uniquement pour l'adresse IP du module Onboard Administrator actuel. Si vous modifiez l'adresse IP, le paramètre doit être appliqué à nouveau à partir de la nouvelle adresse.) Pour vous assurer que toutes les pages de l'interface utilisateur du module Onboard Administrator héritent de la langue sélectionnée, cliquez sur **Refresh** (Actualiser) en bas de l'écran User Preferences.

Chacun de ces paramètres est spécifique au navigateur. Par exemple, un paramètre de langue pour Internet Explorer n'affecte pas le paramètre de Firefox. Vous n'avez pas à utiliser la même méthode sur tous les navigateurs. Après avoir configuré votre langue préférée, afin que le paramètre devienne effectif, vous devrez peut-être actualiser ou recharger la page Web.

REMARQUE : Si le chargement de la langue d'affichage ne s'effectue pas correctement, effacez le cache du navigateur et actualisez l'application en actualisant ou rechargeant le navigateur.

Lorsque vous êtes connecté à un boîtier principal avec des boîtiers liés, assurez-vous que tous les boîtiers liés ont une version compatible du module de langue installé.

Journal système

Le journal système affiche les informations consignées d'événements survenus dans le module Onboard Administrator.

Les événements sont consignés du début à la fin de la liste, l'événement consigné le plus récent étant placé en début de liste. Vous pouvez faire défiler le contenu du journal système à l'aide de la barre de défilement située dans la partie droite de l'écran du journal (si le journal est plus large que la zone d'affichage).

Le journal a une capacité maximale d'environ 18 Ko. Lorsque le journal atteint cette capacité, il supprime automatiquement l'événement enregistré le plus ancien en premier (premier entré, premier sorti).

Pour effacer la liste de tous les événements consignés dans le journal système, cliquez sur le bouton **Clear Log** (Effacer journal) situé dans la partie inférieure droite sous l'affichage du journal système.

Journal système étendu

Le module Onboard Administrator enregistre automatiquement 300 Ko de l'historique le plus récent du journal système. Ce journal système étendu est conservé pendant un réamorçage, un redémarrage et une mise hors tension, si ces actions sont effectuées de manière ordonnée. Dans des circonstances optimales, le module Onboard Administrator enregistre automatiquement jusqu'à 400 Ko de l'historique le plus récent du journal système. Si l'alimentation du module Onboard Administrator est supprimée de manière inattendue ou que le module Onboard Administrator est retiré du boîtier sans un arrêt adéquat, les parties les plus récentes (non enregistrées) du journal système étendu peuvent être perdues.

Pour afficher le journal système étendu, utilisez la commande `SHOW SYSLOG HISTORY` de l'interface CLI.

Consignation de système distant

Vous pouvez utiliser la consignation d'événements du système distant pour envoyer des messages syslog du module Onboard Administrator à un serveur distant sur le réseau pour un stockage continu. Pour configurer cette fonction, utilisez l'onglet Log Options (Onglet Log Options à la page 227).

Onglet Log Options

Cet écran permet d'envoyer des messages du journal système à un serveur distant sur le réseau pour un stockage continu. Par défaut, la consignation du système local est activée. Pour gérer les paramètres du journal système, vous devez être un administrateur ou un opérateur doté de permissions de baie de module OA.

Les messages syslog sont envoyés du module Onboard Administrator à l'aide du protocole UDP sur un port qui peut être spécifié par l'utilisateur. Le port syslog à distance par défaut est 514.

La fonctionnalité de consignation des événements du système distant des modules Onboard Administrator est conforme aux directives RFC3164 (http://www.ietf.org/rfc/rfc3164.txt).

Sur la plupart des systèmes Linux, la consignation des événements du système distant peut être activée en démarrant syslog avec l'option « -r ». Le port syslog à distance doit être ouvert également dans le pare-feu. Pour plus d'informations, reportez-vous à la documentation de votre distribution spécifique. Les systèmes d'exploitation Windows® ne proposent aucune prise en charge native pour la consignation d'événements de système distant. Toute application qui écoute sur le port UDP 514 ou sur le port syslog spécifié peut recevoir des messages du journal du système distant du module OA.

Pour envoyer des messages du journal système à un hôte distant, cochez la case **Enable remote system logging** (Activer la consignation du système distant). Spécifiez le serveur et le port.

Une fois configurée, la fonction de consignation du système distant du module Onboard Administrator peut être testée à l'aide du bouton Test de l'interface graphique ou via la commande `TEST SYSLOG` de l'interface CLI.

Champ	Valeur possible	Description
Syslog Server Address (Adresse du serveur syslog)	• Adresse IPv4 : ###.###.###.### où ### est compris entre 0 et 255. • Adresse Ipv6 : ####:####:####:####:####:####:####:#### où #### est compris entre 0 et FFFF. • Nom DNS : peut comprendre entre 1 et 64 caractères notamment tous les caractères alphanumériques et le tiret (-)	Une adresse IPv4, une adresse IPv6 ou le nom DNS de l'hôte distant*
Port	Entier compris entre 1 et 65535	Port IP de l'hôte distant.

* Utilisez une adresse IPv6 comme serveur de consignation du système distant.

Pour envoyer un message de test à l'adresse de l'hôte distant et au journal système local, cliquez sur **Test Remote Log** (Tester la consignation distante). Pour utiliser cette fonction, vous devez activer la consignation du système distant.

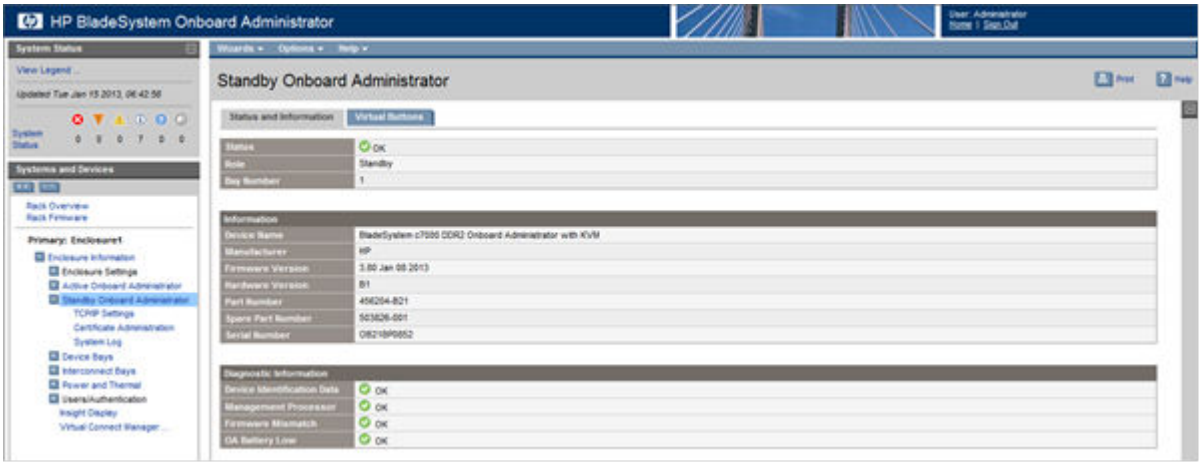
Pour enregistrer les paramètres, cliquez sur **Apply** (Appliquer).

Module Onboard Administrator en mode Standby

Écran Standby Onboard Administrator

Lorsqu'un second module Onboard Administrator est placé dans le boîtier, il devient le module Onboard Administrator en mode Standby. Le module Onboard Administrator en mode Standby est normalement placé dans le plateau Onboard Administrator disponible à l'arrière du boîtier. En sélectionnant l'écran Active to Standby (Actif à mode Standby), vous pouvez forcer une transition dans l'interface utilisateur du module Onboard Administrator pour faire en sorte que le module Onboard Administrator actif devienne le module Onboard Administrator en mode Standby.

Pour une relation active/mode Standby, la même version de microprogramme doit être installée pour les deux modules Onboard Administrator. Si les versions du microprogramme ne sont pas identiques, l'écran Insight Display et l'écran d'état principal du module Onboard Administrator identifient cette erreur et alertent l'utilisateur via SNMP s'il est activé.



Si vous utilisez deux modules Onboard Administrator, chacun d'eux utilise une adresse IP unique. Reportez-vous à l'écran Insight Display pour obtenir les adresses IP des modules Onboard Administrator actif et en mode Standby et prenez note de ces adresses. Lorsque vous examinez le boîtier de l'arrière, la baie située à gauche est la baie 1, tandis que la baie située à droite est la baie 2. Lors de la transition du module Onboard Administrator actif vers le module Onboard Administrator en mode Standby, le nom d'hôte DNS et les adresses IP restent les mêmes. Pour vous connecter au nouveau module Onboard Administrator actif, vous devez fermer complètement votre navigateur et vous connecter au nom d'hôte ou à l'adresse IP de l'ancien module Onboard Administrator en mode Standby.

Onglets Status, Information et Virtual Buttons

Les informations présentées dans les onglets Status (État), Information (Informations) et Virtual Buttons (Boutons virtuels) sont identiques à celles d'un module Onboard Administrator actif. Pour plus d'informations sur ces onglets, consultez la section « Écran Active Onboard Administrator » (Écran Active Onboard Administrator à la page 207).

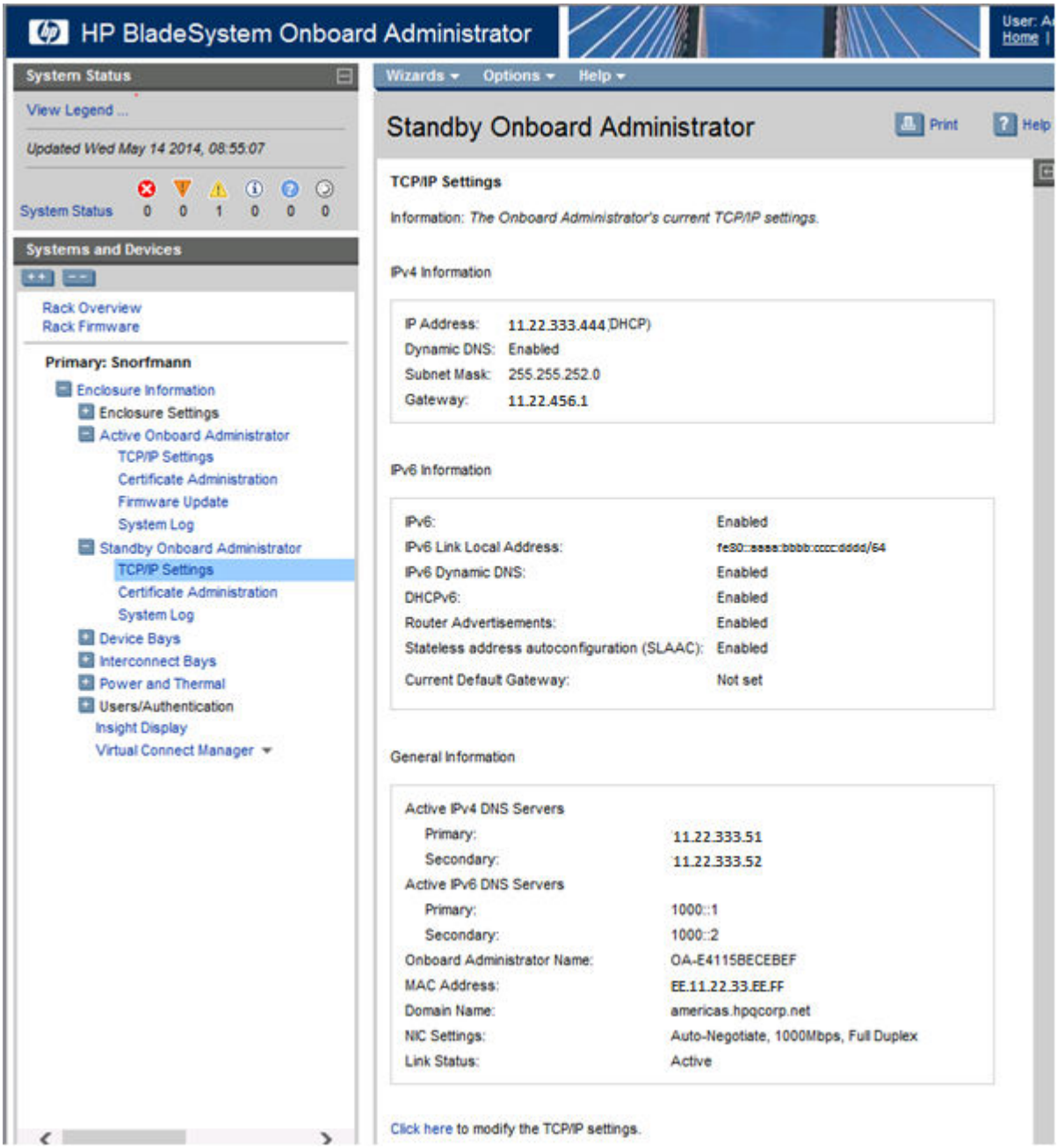
Lorsqu'un câble réseau est connecté au module Onboard Administrator en Standby ou en est déconnecté, une interruption SNMP (si activée) identifiant le changement d'état de la liaison réseau correspondante est envoyée par le module Onboard Administrator actif.

Onglet Virtual Buttons du module Onboard Administrator en mode Standby

Cliquez sur **Reset** (Réinitialiser) pour réinitialiser le module Onboard Administrator. Un écran de confirmation s'affiche, vous invitant à confirmer que vous souhaitez exécuter l'action et vous indiquant que vous serez déconnecté du module Onboard Administrator. Cliquez sur **OK** pour continuer, ou sur **Cancel** (Annuler) pour quitter sans apporter de modification.

Cliquez sur **Toggle On/Off** (Activé/Désactivé) pour modifier le voyant d'UID du module Onboard Administrator. Ceci identifie un module Onboard Administrator spécifique lorsqu'il en existe plusieurs.

Paramètres TCP/IP pour module OA en Standby, vu du module OA actif



Cet écran, comme illustré dans l'interface utilisateur du module Onboard Administrator actif, affiche les paramètres TCP/IP du boîtier actuel pour le module Onboard Administrator en Standby.

Pour plus d'informations sur les paramètres TCP/IP affichés dans cet écran, consultez l'écran Active Onboard Administrator TCP/IP Settings (Écran TCP/IP Settings du module Onboard Administrator actif à la page 211).

Pour modifier les paramètres TCP/IP, sélectionnez **Click here** (Cliquer ici). Pour plus d'informations sur les paramètres TCP/IP que vous pouvez modifier, consultez l'écran Enclosure TCP/IP Settings (Paramètres TCP/IP du boîtier à la page 126).

Paramètres TCP/IP en Standby affichés à partir de l'interface du module Onboard Administrator en Standby

L'écran de paramètres TCP/IP vu à partir de l'interface du module Onboard Administrator en Standby affiche quatre onglets :

- IPv4 Settings
- IPv6 Settings
- NIC Options
- Advanced Settings

Ces onglets affichent les paramètres visibles dans l'exemple d'écran précédent, mais permettent également de modifier la plupart des paramètres directement.

Les onglets IPv4 Settings et IPv6 Settings permettent de modifier la plupart des paramètres modifiables à partir des onglets correspondants sur l'écran de paramètres TCP/IP du boîtier dans l'interface utilisateur du module Onboard Administrator actif. Les exceptions sont décrites dans les sections qui suivent. Les onglets NIC Options et Advanced Settings permettent de modifier les mêmes paramètres qui peuvent être modifiés dans les onglets correspondants sur l'écran de paramètres TCP/IP du boîtier dans l'interface utilisateur du module Onboard Administrator actif.

Exceptions concernant les paramètres IPv4

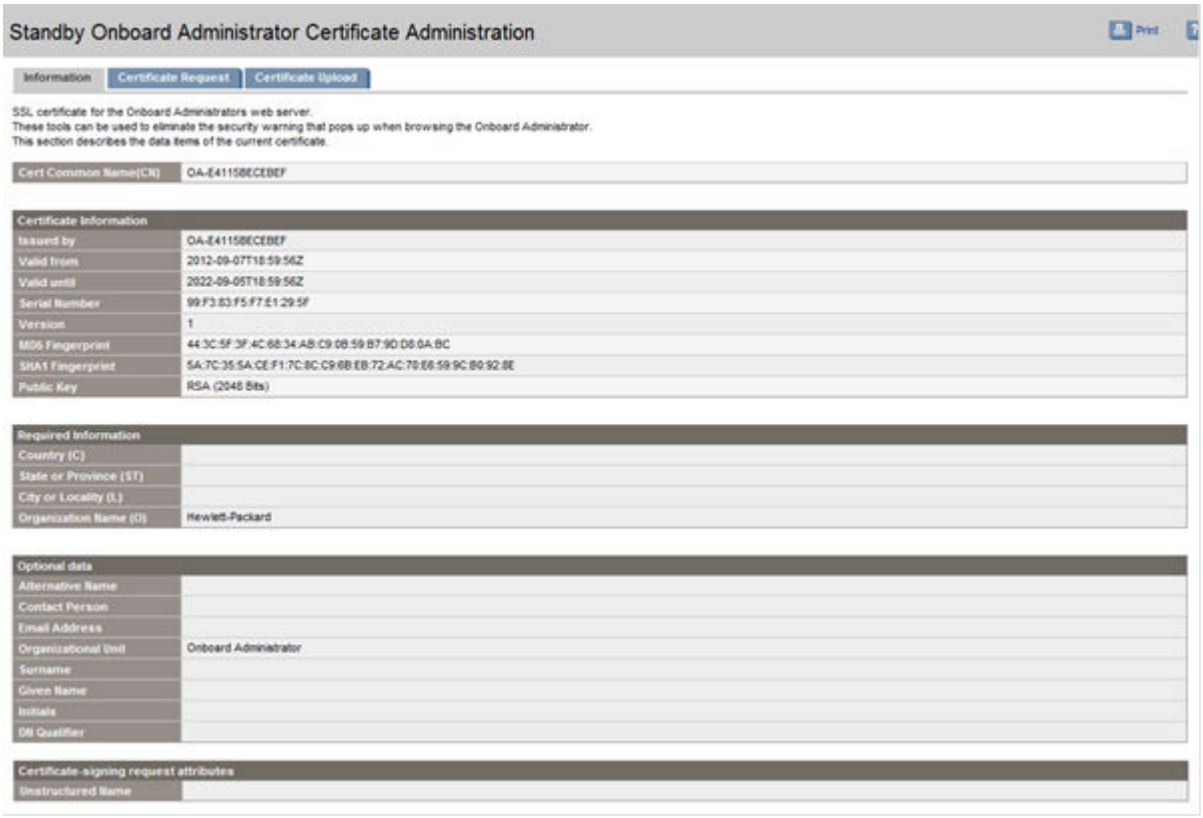
Vous ne pouvez pas modifier le paramètre **Enclosure IP Mode** (Mode IP du boîtier) à partir de l'interface du module Onboard Administrator en Standby. Modifiez-le à partir de l'onglet IPv4 Settings des paramètres TCP/IP du boîtier dans l'interface utilisateur du module Onboard Administrator actif (Onglet IPv4 Settings à la page 126).

Exceptions concernant les paramètres IPv6

Vous ne pouvez pas modifier les paramètres suivants à partir de l'interface du module Onboard Administrator en Standby. Modifiez-le à partir de l'onglet IPv6 Settings des paramètres TCP/IP du boîtier dans l'interface utilisateur du module Onboard Administrator actif (Onglet IPv6 Settings à la page 129).

- **Mode IP du boîtier**
- **Activer IPv6**
- **Activer annonces de routeur**
- **Activer SLAAC**
- **Activer DHCPv6**

Onglet Standby Onboard Administrator Certificate Administration Information



Onglet Informations

Cet écran affiche des informations détaillées concernant le certificat SSL actuellement utilisé par le module Onboard Administrator. Un certificat SSL est utilisé pour certifier l'identité du module Onboard Administrator et est requis par le serveur HTTP sous-jacent pour établir un canal de communications sécurisé (crypté) avec le navigateur Web du client.

Au démarrage initial, le module Onboard Administrator génère un certificat SSL auto-signé par défaut valide pour 10 ans, et le certificat est émis au nom du module Onboard Administrator. Dans la mesure où ce certificat par défaut est auto-signé, le champ « Issued by » (Émis par) est également défini sur le même nom.

Informations d'état

Rangée	Description
Cert Common Name	Nom commun de l'objet du certificat.

Informations sur le certificat

Rangée	Description
Issued by (Émis par)	Autorité de certification qui a émis le certificat
Valid from (Valide à partir de)	Date à partir de laquelle le certificat est valide
Valid until (Valide jusqu'à)	Date à laquelle le certificat expire

Rangée	Description
Serial Number (Numéro de série)	Numéro de série attribué au certificat par l'autorité de certification
Version	Numéro de version du certificat actuel
MD5 Fingerprint (Empreinte MD5)	Ce champ est une validation d'authenticité et est incorporé dans le certificat
SHA1 Fingerprint (Empreinte SHA1)	Ce champ est une validation d'authenticité et est incorporé dans le certificat
Public Key (Clé publique)	Nom de la clé publique.

Informations requises

Rangée	Description
Country (C) (Pays)	Code de pays à deux caractères qui identifie le pays dans lequel le module Onboard Administrator est situé.
State or Province (ST) (État ou province)	État ou province dans lequel/laquelle est installé le module Onboard Administrator.
City or Locality (L) (Ville ou localité)	Ville ou localité dans laquelle est installé le module Onboard Administrator.
Organization Name (O) (Nom d'organisation)	Société qui possède ce module Onboard Administrator.

Données facultatives

Rangée	Description
Alternative Name (Nom secondaire)	Autre nom du module Onboard Administrator.
Contact Person (Contact)	Personne responsable du module Onboard Administrator.
Email Address (Adresse électronique)	Adresse électronique de la personne responsable du module Onboard Administrator.
Organizational Unit (Unité organisationnelle)	Unité, au sein de l'entreprise ou de l'organisation, qui possède le module Onboard Administrator.
Surname (Nom)	Nom de famille de la personne responsable du module Onboard Administrator.
Given Name (Prénom)	Prénom de la personne responsable du module Onboard Administrator.
Initials (Initiales)	Initiales de la personne responsable du module Onboard Administrator.
DN Qualifier (Qualificatif de nom distinctif)	Qualificatif de nom distinctif du module Onboard Administrator.

Attributs de demande de signature de certificat

Rangée	Description
Unstructured Name (Nom non structuré)	Destiné à des informations supplémentaires.

Onglet Standby Certificate Request

L'onglet Standby Certificate Request (Demande de certificat en mode Standby) permet d'entrer les informations requises pour générer un certificat auto-signé ou une demande de signature de certificat normalisé vers une autorité de certificats.

Informations requises

Champ	Valeurs possibles	Description
Country (C) (Pays)	Doit être un code de pays à deux caractères. Les caractères autorisés sont tous les caractères alphanumériques, les espaces et les signes de ponctuation suivants : ' ( ) + , - . / : = ?	Code de pays à deux caractères qui identifie le pays dans lequel le module Onboard Administrator est situé.
State or Province (ST) (État ou province)	Doit comporter entre 1 et 30 caractères.	État ou province dans lequel/laquelle est installé le module Onboard Administrator.
City or Locality (L) (Ville ou localité)	Doit comporter entre 1 et 50 caractères.	Ville ou localité dans laquelle est installé le module Onboard Administrator.
Organization Name (O) (Nom d'organisation)	Doit comporter entre 1 et 60 caractères.	Organisation qui possède ce module Onboard Administrator. Lorsque cette information est utilisée pour générer une requête de signature de certificat, l'autorité délivrant le certificat peut vérifier que l'organisation demandeuse est effectivement en droit de se déclarer propriétaire de ladite organisation ou entreprise.
Common Name (CN) (Nom commun)	Doit comporter entre 1 et 60 caractères. Pour éviter des alertes de sécurité, la valeur de ce champ doit correspondre exactement au nom d'hôte tel qu'il est connu par le navigateur Web. Le navigateur Web compare le nom d'hôte apparaissant dans l'adresse Web résolue avec celui spécifié dans le certificat. Par exemple, si l'adresse Web dans le champ d'adresse est https://oa-001635.xyz.com, la valeur doit être oa-001635.xyz.com.	Nom du module Onboard Administrator indiqué dans le champ d'adresse Web. Cet attribut de certificat est plus connu sous le nom de nom commun.

Pour inclure une demande de certificat pour un module Onboard Administrator actif, sélectionnez **Active OA Host Name**. Entrez les informations dans le champ **Active Common Name (CN)**, avec une longueur comprise entre 1 et 60 caractères.

Informations facultatives

Champ	Valeurs possibles	Description
Alternative Name (Nom secondaire)	Doit comporter entre 0 et 511 caractères.	Autre nom du module Onboard Administrator. Le nom est utilisé pour la création de l'attribut d'extension du nom d'objet secondaire X509v3. Le champ doit soit être vide soit contenir une liste de paires mot-clé-valeur séparées par des virgules. Les entrées mot-clé-valeur valides incluent IP:<adresse_ip> et DNS:<nom_domaine>.
Contact Person (Contact)	Doit comporter entre 0 et 60 caractères.	Personne responsable du module Onboard Administrator.
Email Address (Adresse électronique)	Doit comporter entre 0 et 60 caractères.	Adresse e-mail de la personne responsable du module Onboard Administrator.
Organizational Unit (Unité organisationnelle)	Doit comporter entre 0 et 60 caractères.	Unité, au sein de l'entreprise ou de l'organisation, qui possède le module Onboard Administrator.
Surname (Nom)	Doit comporter entre 0 et 60 caractères.	Nom de famille de la personne responsable du module Onboard Administrator.
Given Name (Prénom)	Doit comporter entre 0 et 60 caractères.	Prénom de la personne responsable du module Onboard Administrator.
Initials (Initiales)	Doit comporter entre 0 et 20 caractères.	Initiales de la personne responsable du module Onboard Administrator.
DN Qualifier (Qualificatif de nom distinctif)	Doit comporter entre 0 et 60 caractères. Les caractères autorisés sont tous les caractères alphanumériques, les espaces et les signes de ponctuation suivants : ' ( ) + , - . / : = ?	Qualificatif de nom distinctif du module Onboard Administrator.

Attributs de demande de signature de certificat

Champ	Valeurs possibles	Description
Challenge Password (Mot de passe)	Longueur comprise entre 0 et 30 caractères	Mot de passe de demande de signature du certificat
Confirm Password (Confirmer le mot de passe)	Longueur comprise entre 0 et 30 caractères	Confirmation du mot de passe
Unstructured Name (Nom non structuré)	Longueur comprise entre 0 et 60 caractères	Destiné à des informations supplémentaires comme, par exemple, un nom non structuré qui est attribué au module Onboard Administrator

Cliquez sur **Apply** (Appliquer) pour générer un certificat auto-signé ou une demande de signature de certificat normalisé.

Demande de signature de certificat normalisé

Cet écran affiche une demande de signature de certificat normalisé générée par le module Onboard Administrator. Le contenu de la demande dans la zone de texte peut être envoyé à une autorité de

certification de votre choix pour signature. Une fois signé et renvoyé par l'autorité de certification, le certificat peut être téléchargé sous l'onglet Certificate Upload (Téléchargement de certificat).

Si une adresse IP statique est configurée pour le module Onboard Administrator lorsque cette demande de certificat est générée, cette dernière sera émise vers l'adresse IP statique. Sinon, elle est émise vers le nom DNS dynamique du module Onboard Administrator. Par défaut, le certificat demande une durée de validité de 10 ans (cette valeur n'est actuellement pas configurable).

Lorsque vous soumettez la demande à l'autorité de certification, assurez-vous :

1. D'utiliser l'URL du module Onboard Administrator pour le serveur.
2. De demander que le certificat soit généré au format RAW.
3. D'inclure les lignes Begin (Début) et End (Fin) du certificat.

Onglet Standby Certificate Upload

Vous pouvez utiliser deux méthodes pour télécharger des certificats en vue de les utiliser dans le module HP BladeSystem Onboard Administrator :

- Collez le contenu du certificat dans la zone de texte et sélectionnez **Upload** (Télécharger).
- Collez l'URL complète du certificat dans le champ URL et sélectionnez **Apply** (Appliquer).

Le certificat à télécharger doit provenir d'une demande de certificat envoyée et signée par une autorité de certification pour ce module Onboard Administrator donné. Sinon, le certificat ne correspond pas aux clés privées utilisées pour générer la demande de certificat, et le certificat est rejeté. En outre, si le domaine du module Onboard Administrator a été détruit ou réimporté, vous devrez à nouveau répéter la procédure de génération d'une demande de certificat. Il sera signé par une autorité de certification car les clés privées sont détruites et recréées ainsi que le domaine du module Onboard Administrator.

Si le nouveau certificat est accepté et installé avec succès par le module Onboard Administrator, vous êtes automatiquement déconnecté. Le serveur HTTP doit être redémarré pour que le nouveau certificat prenne effet.

Pour plus d'informations sur la sous-catégorie System Log, consultez la section « Journal système » (Journal système à la page 227).

Journal système pour module Onboard Administrator en Standby

Le journal système affiche les informations consignées d'événements survenus dans le module Onboard Administrator.

Les événements sont consignés du haut de la liste jusqu'au bas, l'événement consigné le plus récent apparaissant au bas de la liste. Si la liste est plus longue que la zone d'affichage, vous pouvez la faire défiler à l'aide de la barre de défilement sur le côté droit de l'écran du journal.

Lorsque le journal atteint la capacité maximum, il supprime automatiquement l'événement consigné le plus ancien en premier (premier entré, premier sorti).

Pour effacer la liste de tous les événements consignés, cliquez sur **ClearLog** (Effacer journal), sous l'affichage du journal système.

Standby à Actif

Pour forcer le module Onboard Administrator en mode Standby à passer en mode Actif, cliquez sur **Transition Standby to Active**. Un écran de confirmation s'affiche, vous invitant à confirmer l'action.

Pour continuer, cliquez sur **OK**. Pour quitter sans apporter de modification, cliquez sur **Cancel** (Annuler).

Cette fonctionnalité est uniquement disponible lorsque vous êtes connecté à l'interface utilisateur du module Onboard Administrator en Standby.

Vous pouvez également forcer le module Onboard Administrator à passer en mode Actif à l'aide de la commande FORCE TAKEOVER de l'interface CLI.

Le temps de transition du mode actif au mode Standby et inversement varie en fonction de la configuration, du remplissage du boîtier et de divers autres facteurs. Le retrait du module Onboard Administrator précédemment actif au début du processus de transition oblige le temps de transition du passage de l'état Standby à l'état Actif à augmenter.

Baies de périphérique

Baies de périphérique

Résumé de baies de périphérique

Dans le menu Systems and Devices (Systèmes et périphériques), la catégorie Device Bays (Baies de périphérique) répertorie toutes les lames du boîtier. La sélection de Device Bays dans le menu affiche la liste des périphériques, avec une grille présentant l'état de chaque lame dans le boîtier.

La case à cocher dans la première colonne sur la ligne supérieure bascule toutes les cases à cocher pour toutes les lames dans le boîtier, ce qui permet de mettre sous ou hors tension toutes les lames de serveur dans le boîtier. Au besoin, vous pouvez utiliser des cases à cocher individuelles pour sélectionner une lame spécifique. Une fois les lames sélectionnées, choisissez Virtual Power (Alimentation virtuelle), UID state (État de l'UID), One Time Boot (Démarrage ponctuel), DVD ou Enclosure Firmware Management (Gestion des microprogrammes du boîtier) dans les menus, selon l'action à réaliser. Les commandes virtuelles ne sont pas applicables aux lames de stockage.

Liste des périphériques

Colonne	Description
Case à cocher	Cochez la case des baies auxquelles appliquer l'action Virtual Power, UID State, One Time Boot, DVD ou Firmware Management.
Bay (Baie)	Baie du périphérique dans le boîtier.
Status (État)	État global du périphérique. Les valeurs possibles sont OK et Enclosure Firmware Management.
UID	État de l'UID sur le périphérique. Les valeurs possibles sont On (Activé, en bleu), Off (Désactivé, en gris) et Blink (Clignotement). Lorsque le voyant d'UID clignote, une opération critique est en cours d'exécution sur le périphérique qu'il convient de ne pas interrompre.
Power State (État de l'alimentation)	État d'alimentation du périphérique. Les valeurs possibles sont On (Activé) et Off (Désactivé).
iLO IP Address (Adresse IP de iLO)	Adresse IP de l'iLO dans la lame de serveur. Non applicable pour les lames de stockage. Pour vous connecter à iLO, cliquez sur le lien d'adresse IP. Pour afficher tous les liens d'adresse IP de carte iLO disponibles, cliquez sur la flèche vers le bas sur la droite de l'adresse IP de carte iLO. Une fenêtre contextuelle affiche les

Colonne	Description
	liens d'adresse Web que vous pouvez utiliser pour vous connecter à la carte iLO. Si la prise en charge du lien FQDN est activée et que certaines exigences de configuration DNS sont remplies, une adresse Web basée sur le nom de domaine complet est la sélection par défaut. Pour plus d'informations sur l'activation de la prise en charge du lien FQDN, consultez la page « Accès réseau ».
iLO Name (Nom de l'iLO)	Nom DNS de l'iLO dans la lame de serveur. Non applicable pour les lames de stockage.
iLO DVD Status (État de DVD iLO)	État de la connexion de DVD à la lame de serveur. Les valeurs possibles sont Connected (Connecté), Disconnected (Déconnecté) ou Unknown (Inconnu). Un état Incompatible Firmware (Microprogramme incompatible) indique que la fonctionnalité DVD n'est pas prise en charge avec le microprogramme iLO installé sur le périphérique. Un état Unknown (Inconnu) indique la présence d'un problème de connectivité iLO.

Les informations sur cette page sont actuelles à l'heure du dernier téléchargement. Pour visualiser des informations mises à jour, cliquez sur **Refresh** (Actualiser).

UID State (État UID)

Le menu déroulant UID State (État de l'UID) permet de définir l'état du voyant d'UID sur les lames. L'activation du voyant d'UID permet de localiser plus facilement une lame spécifique dans un boîtier. Vous pouvez activer ou désactiver ces voyants d'UID individuellement ou en groupes, selon les cases à cocher sélectionnées.

Virtual Power

Les commandes d'alimentation virtuelle ne sont pas applicables aux lames partenaires.

Bouton	Description
Momentary Press (Pression momentanée)	Ce bouton réplique une pression momentanée physique du bouton d'alimentation sur la lame de serveur. Un clic sur ce bouton met sous ou hors tension la lame de serveur de manière ordonnée.
Press and Hold (Appuyer et maintenir enfoncé)	Ce bouton réplique une pression physique et un maintien enfoncé du bouton d'alimentation sur la lame de serveur. Un clic sur ce bouton force la mise hors tension de la lame de serveur sans mise hors tension préalable du système d'exploitation. Cette option n'est pas disponible lorsque la lame de serveur est hors tension.
Cold Boot (Démarrage à froid)	Un clic sur ce bouton supprime immédiatement l'alimentation du système. Cette option n'est pas disponible lorsque la lame de serveur est hors tension.
Reset (Réinitialiser)	Un clic sur ce bouton effectue une réinitialisation du système. Cette option n'est pas disponible lorsque la lame de serveur est hors tension.

One Time Boot (Démarrage unique)

Si Secure Boot est en vigueur sur la lame dans une baie sélectionnée, cette opération ne peut pas être effectuée à partir de l'interface CLI ou de l'interface utilisateur du module Onboard Administrator. Elle peut être effectuée uniquement à partir du périphérique configuré dans le BIOS par l'administrateur.

Si vous spécifiez des paramètres de démarrage unique, ceux-ci sont valides uniquement pour le prochain réamorçage de la lame de serveur. Une fois que l'amorçage est terminé, la lame de serveur utilise les paramètres par défaut pour les redémarrages suivants.

Option	Description
No one time Boot (Pas de démarrage unique)	Force la lame de serveur à effacer les paramètres de démarrage unique.
Diskette Drive (A:) (Lecteur de disquette (A:))	Force la lame de serveur à redémarrer à partir du lecteur de disquette. Vérifiez que le lecteur de disquette est connecté à la lame de serveur avant de sélectionner cette option.
CD-ROM	Force la lame de serveur à redémarrer à partir du lecteur de CD-ROM. Vérifiez que le lecteur de CD-ROM est connecté à la lame de serveur avant de sélectionner cette option.
Hard Drive C: (Disque dur C:)	Force la lame de serveur à redémarrer à partir du disque dur.
RBSU	Force la lame de serveur à démarrer sur l'outil ROM-Based Setup Utility.
PXE NIC	Force la lame de serveur à démarrer à partir de la carte réseau PXE.
USB	Force la lame de serveur à démarrer à partir de la clé USB.
Embedded UEFI Shell (Shell UEFI intégré)	Force la lame de serveur à démarrer à partir du shell UEFI intégré. Cette option est grisée si plusieurs serveurs sont sélectionnés ou si le serveur sélectionné n'est pas un serveur compatible UEFI.
UEFI Target (cible UEFI)	Force la lame de serveur à démarrer à partir du périphérique cible UEFI. Cette opération peut être effectuée uniquement sur un serveur, après sélection de celui-ci. Cette option est grisée si plusieurs serveurs sont sélectionnés, ou si le serveur sélectionné n'est pas un serveur compatible UEFI ou est un serveur compatible UEFI en mode d'amorçage BIOS hérité.

DVD

Le menu DVD permet de connecter ou déconnecter l'unité de DVD partagée en sélectionnant **Connect to Enclosure DVD** (Connecter au DVD du boîtier) ou **Disconnect DVD Hardware** (Déconnecter matériel DVD). Vous pouvez connecter le lecteur de DVD partagé à plusieurs lames de serveur. Une fois le lecteur de DVD partagé connecté, vous pouvez utiliser le menu Virtual Power pour redémarrer les lames de serveur sélectionnées dans la liste. Si plusieurs disques de support sont requis pour une installation, vous pouvez avoir à effectuer une déconnexion, puis une reconnexion pour chaque serveur lors de l'insertion du nouveau disque de support dans le lecteur de DVD.

Lorsqu'une clé USB est détectée sur le port USB du module Onboard Administrator actif et que des images ISO sont présentes, ces éléments apparaissent dans le menu DVD. Sélectionnez les lames de serveur vers lesquelles vous souhaitez déployer une image ISO, puis sélectionnez l'image ISO dans le menu. L'image ISO est déployée.

Enclosure Firmware Management

Il est possible d'effectuer une opération de détection manuelle sur un ou plusieurs serveurs pour simplifier la collecte des versions des microprogrammes installés.

Lorsqu'on lance une opération manuelle de détection des microprogrammes, un écran de sélection des baies de périphériques s'affiche. Sélectionnez une ou plusieurs baies de périphérique sur lesquelles effectuer la détection ou cochez la case **Discover All Servers** (Détecter tous les serveurs). Toutes les baies de périphériques et la case Discover All Servers sont sélectionnées par défaut.

Si le mode Secure Boot est configuré sur une lame de serveur, vous ne pouvez pas sélectionner la baie associée (une icône de cadenas est affichée). Le mode Secure Boot empêche les utilisateurs d'effectuer une détection manuelle à partir de l'interface CLI ou de l'interface utilisateur du module Onboard Administrator. Les opérations d'amorçage peuvent être effectuées uniquement à partir du périphérique d'amorçage configuré dans le BIOS par l'administrateur.

Pour lancer le processus de découverte sur le serveur sélectionné, cliquez sur **Start Manual Discovery** (Lancer la découverte manuelle).

Une mise à jour manuelle d'un ou de plusieurs serveurs vers les versions d'image des microprogrammes désignées peut être initiée. Pour lancer une mise à jour des microprogrammes sur un ou plusieurs serveurs, cliquez sur **Manual Update** (Mise à jour manuelle).

Lorsqu'on lance une opération manuelle de mise à jour des microprogrammes, un écran de sélection des baies de périphériques s'affiche. Sélectionnez une ou plusieurs baies de périphériques sur lesquelles effectuer la mise à jour ou cochez la case **Update All Servers** (Mettre à jour tous les serveurs) pour sélectionner tous les serveurs pour la mise à jour. Toutes les baies de périphériques et la case Discover All Servers sont sélectionnées par défaut.

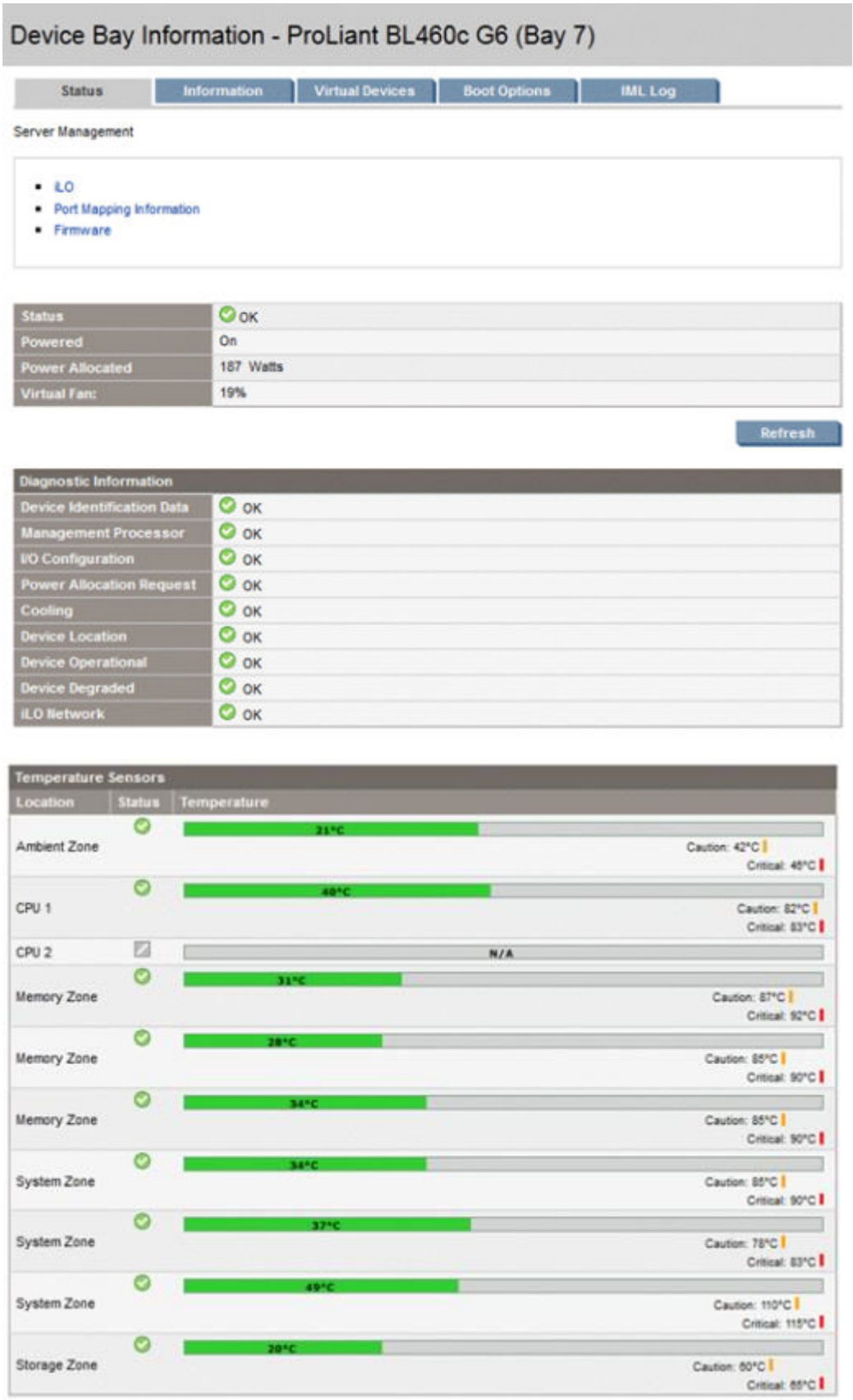
Si le mode Secure Boot est configuré sur une lame de serveur, vous ne pouvez pas sélectionner la baie associée (une icône de cadenas est affichée). Le mode Secure Boot empêche les utilisateurs d'effectuer une mise à jour manuelle à partir de l'interface CLI ou de l'interface utilisateur du module Onboard Administrator. Les opérations d'amorçage peuvent être effectuées uniquement à partir du périphérique d'amorçage configuré dans le BIOS par l'administrateur.

Pour lancer le processus de mise à jour sur le serveur sélectionné, cliquez sur **Start Manual Update** (Lancer la mise à jour manuelle).

Onglet Device Bay Status

La sélection d'une lame spécifique du boîtier affiche l'écran Device Bay Information pour la baie *xx*, où *xx* est la baie sélectionnée. Cet écran fournit des onglets pour les catégories Status (État), Information, Virtual Devices (Périphériques virtuels), Boot Options (Options de démarrage) et IML Log (Journal IML).

La section Server Management (Gestion du serveur) de la page contient des liens destinés à vous aider à superviser la lame de serveur dans la baie de périphérique.


Device Bay Information - ProLiant BL460c G6 (Bay 7)
Status
Information
Virtual Devices
Boot Options
IML Log
Server Management
iLO
Port Mapping Information
Firmware
Status
OK
Powered
On
Power Allocated
187 Watts
Virtual Fan:
19%
Refresh
Diagnostic Information
Device Identification Data
OK
Management Processor
OK
I/O Configuration
OK
Power Allocation Request
OK
Cooling
OK
Device Location
OK
Device Operational
OK
Device Degraded
OK
iLO Network
OK
Temperature Sensors
Location
Status
Temperature
Ambient Zone
21°C
Caution: 42°C
Critical: 46°C
CPU 1
40°C
Caution: 82°C
Critical: 83°C
CPU 2
N/A
Memory Zone
31°C
Caution: 87°C
Critical: 92°C
Memory Zone
28°C
Caution: 85°C
Critical: 90°C
Memory Zone
34°C
Caution: 85°C
Critical: 90°C
System Zone
34°C
Caution: 85°C
Critical: 90°C
System Zone
37°C
Caution: 78°C
Critical: 83°C
System Zone
49°C
Caution: 110°C
Critical: 115°C
Storage Zone
28°C
Caution: 60°C
Critical: 65°C

Rangée	Description
System Event Health (Intégrité des événements système)	Intégrité des événements système internes que signale le périphérique. Si l'état n'est pas OK, examinez le journal des événements système de la lame sur l'iLO pour déterminer la cause de la condition. Les valeurs possibles sont OK, Degraded (Détérioré) et Failed (Échec).
Status (État)	État global de la lame. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Dégradé), Failed (En échec) ou Other (Autre) avec une icône d'information. L'icône d'information avec un état Other s'affiche jusqu'à ce que la lame de serveur soit configurée pour Virtual Connect Manager. Pour plus d'informations, voir le tableau Diagnostic Information (Informations de diagnostic).
Powered (Alimentée)	État d'alimentation de la lame. Les valeurs possibles sont On (Activé) et Off (Désactivé).
Power Delay Remaining (Délai restant avant alimentation)	Temps restant en secondes avant la mise sous tension du périphérique.
Power Allocated (Puissance allouée)	Puissance d'alimentation autorisée pour la lame, en watts.
Partner Device (Périphérique partenaire)	Lame de stockage/extension à laquelle est associée la lame de serveur. Ces informations ne s'affichent pas en cas d'absence de périphérique partenaire.
Virtual Fan (Ventilateur virtuel)	Pourcentage de la vitesse maximum (RPM) du ventilateur virtuel.

Informations de diagnostics

Rangée	Description
Device Identification Data (Données d'identification du périphérique)	Nom du modèle, référence, numéro de série et autres informations utilisées pour identifier le périphérique. Ces données sont également appelées données FRU. Une erreur de données d'identification du périphérique s'affiche si les données sont absentes ou illisibles par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Management Processor (Processeur de gestion)	État du iLO. Les valeurs possibles sont OK et Error.
Temperature (Température)	La température est au-dessus du seuil d'avertissement. Les valeurs possibles sont OK et Temperature Warning (Avertissement de température).
Overheat Check (Contrôle de surchauffe)	La température est au-dessus du seuil de danger. Les valeurs possibles sont OK et Critical temperature threshold reached (Seuil critique de température atteint).
I/O Configuration (Configuration E/S)	La configuration de la baie de périphérique est incorrecte. Si une lame de stockage est associée à une lame de serveur pleine hauteur, et que la lame de serveur ne dispose pas de la carte mezzanine appropriée, une configuration E/S non valide en résulte. Les valeurs possibles sont OK et I/O mismatch detected (Discordance E/S détectée).
Power Allocation Request (Demande d'allocation d'alimentation)	La puissance disponible est insuffisante pour alimenter correctement cette lame de serveur. Les valeurs possibles sont OK et Insufficient enclosure power (Alimentation de boîtier insuffisante).

Rangée	Description
Cooling (Refroidissement)	Le nombre de ventilateurs est insuffisant pour ventiler correctement cette lame de serveur ou la configuration des ventilateurs est incorrecte. Les valeurs possibles sont OK et Insufficient fans for enclosure cooling (Nombre de ventilateurs insuffisant pour refroidissement du boîtier).
Device Location (Emplacement du périphérique)	La lame de serveur n'a pas été placée dans le bon logement du boîtier d'après la configuration actuelle de ventilation. Les valeurs possibles sont OK et Incorrect location for proper device cooling (Emplacement incorrect pour refroidissement correct du périphérique).
Device Operational (Périphérique fonctionnel)	Le périphérique présente un défaut. L'état n'a pas été demandé par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Device Degraded (Périphérique détérioré)	Le périphérique présente un défaut. L'état a été demandé par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
iLO Network (Réseau iLO)	Détecte un problème de configuration réseau iLO. Les valeurs possibles sont OK ou iLO network configuration problem, check connectivity to iLO default gateway (Problème de configuration réseau iLO, vérifiez la connectivité à la passerelle iLO par défaut). Si le problème persiste, essayez de réinitialiser le système iLO à l'aide de l'interface utilisateur iLO ou de la commande `RESET ILO` de l'interface CLI du module Onboard Administrator. Vous pouvez également utiliser la commande `HPONCFG` de l'interface CLI pour envoyer une commande de script pour réinitialiser iLO.
Memory Error (Erreur de mémoire)	Une erreur de mémoire s'est produite sur la lame de serveur. Pour corriger l'erreur, suivez les instructions fournies.
Mezzanine Card (Carte mezzanine)	Affiche une erreur si une carte mezzanine manquante empêche la lame de serveur d'être associée par partenariat. Affiche OK si aucun problème de partenariat n'a été détecté au cours du diagnostic d'une demande de mise sous tension. Cet état sera réinitialisé en cas de redémarrage du module Onboard Administrator.
Duplicate IP Address (Adresse IP dupliquée)	Coche pour déterminer si une adresse IP dupliquée existe sur le réseau au cours de l'attribution. Les valeurs possibles sont OK ou un message d'informations indiquant s'il existe une adresse IP dupliquée sur le réseau.
Enclosure Dynamic Power Capping (Plafond d'alimentation dynamique du boîtier)	Avertissement signalant que la communication avec l'iLO a été interrompue et qu'aucun plafond d'alimentation ne peut être défini.
Partner Device Link (Lien du périphérique partenaire)	État de liaison du périphérique partenaire de la lame de serveur. Les valeurs possibles sont OK et Inappropriate device in adjacent bay (Périphérique inapproprié dans baie adjacente). Si la lame de serveur n'est pas associée à une lame de stockage, ces informations ne s'affichent pas.
Virtual Connect Configured (Connexion virtuelle configurée)	Les valeurs possibles sont Configured for Virtual Connect (Configurée pour connexion virtuelle) et Not configured for Virtual Connect (Non configurée pour connexion virtuelle). Si la lame de serveur n'est pas configurée pour une connexion virtuelle, une icône d'information avec un état Other s'affiche. Pour configurer le profil de la lame de serveur, accédez à l'outil Virtual Connect Manager.

Rangée	Description
Low Power Request (Demande de faible puissance)	La lame de serveur a signalé une demande d'alimentation anormalement basse. La lame de serveur a été mise hors tension et n'a pas libéré toute la puissance. La lame de serveur continuera à fonctionner correctement, mais corrigez le problème en contactant un représentant de service.
Firmware Management (Gestion du microprogramme)	État de la gestion du microprogramme sur le serveur.
Power Denial-Discovery (Refus d'alimentation-Détection)	Avertissement indiquant que l'alimentation du périphérique a été temporisée durant la recherche de périphériques.
Power Denial-SAS (Refus d'alimentation-SAS)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que le stockage SAS soit prêt.
Power Denial-Partnering (État/contrôle de l'alimentation)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que le périphérique soit configuré pour le partenariat.
Power Denial-VC Profile (Refus d'alimentation-Profil VC)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que le profil VC soit appliqué.
Power Denial-OA Initialization (Refus d'alimentation-Initialisation du module OA)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que le module OA ait terminé l'initialisation.
Power Denial-Power Delay (Refus d'alimentation-Temporisation d'alimentation)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que la temporisation de l'alimentation configurée pour cette baie se soit écoulée.
Power Denial-Firmware Management (Refus d'alimentation-Gestion des microprogrammes)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que le processus de gestion des microprogrammes soit terminé.
Power Denial-I/O Discovery (Refus d'alimentation-Recherche E/S)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que la recherche d'interconnexion soit terminée.
Power Denial-Settings (État/contrôle de l'alimentation)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que les paramètres du périphérique aient été mis à jour. Réessayez l'opération d'alimentation.
Power Denial-Partner Discovery (Refus d'alimentation-Recherche de partenaires)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que les paramètres du périphérique aient été détectés.
Power Denial-I/O Ready (Refus d'alimentation-E/S prêt)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que l'interconnexion correspondante soit prête.
Power Denial-I/O Missing (Refus d'alimentation-Absence E/S)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que l'interconnexion correspondante soit insérée dans le boîtier.
Power Denial-SAS Mezz (Refus d'alimentation-Mezzanine SAS)	Avertissement indiquant que l'alimentation du périphérique a été temporisée jusqu'à ce que la recherche de mezzanine SAS soit terminée.
Power Denial-Blade Link Discovery (Refus d'alimentation-Recherche de liens Blade Link)	Avertissement indiquant que l'alimentation du périphérique a été temporisée durant la recherche de périphériques MMP Blade Link.

Informations de capteurs de température

Colonne	Description
Emplacement	Emplacement du capteur dans le périphérique.
Status (État)	État du capteur de température. L'état correspond à la présentation graphique de la température
Temperature (Température)	Présentation graphique de la température.

iLO

L'iLO pour la lame de serveur dans la baie de périphérique est disponible en cliquant sur **iLO**. La page iLO du module Onboard Administrator s'affiche, comme décrit dans la section « Écran iLO » (Écran iLO à la page 254) de la baie de périphérique.

L'écran iLO de la baie de périphérique propose des liens vers plusieurs interfaces iLO différentes. Lorsque vous cliquez sur un des ces liens, le module Onboard Administrator propose une connexion ponctuelle (dérivation de l'ouverture de session) pour les processeurs de gestion ProLiant iLO. Les niveaux d'accès iLO sont mappés par le niveau de privilège Onboard Administrator (l'utilisateur doit avoir accès à la baie) :

- **Onboard Administrator Administrator** (Administrateur Onboard Administrator) : Administer User Accounts (Administration de comptes utilisateur), Remote Console Access (Accès par console distante), Virtual Power and Reset (Alimentation virtuelle et réinitialisation), Virtual Media (Support virtuel), Configure iLO settings (Configuration des paramètres iLO).
- **Onboard Administrator Operator** (Opérateur Onboard Administrator) : Remote Console Access (Accès par console distante), Virtual Power and Reset (Alimentation virtuelle et réinitialisation), Virtual Media (Support virtuel).

Lorsqu'un utilisateur Onboard Administrator lance l'interface Web iLO ou une console distante iLO, un utilisateur iLO temporaire est créé. Le module Onboard Administrator peut créer jusqu'à trois comptes temporaires pour chaque système iLO. Si un iLO comporte déjà trois comptes Onboard Administrator temporaires ou plus, le module Onboard Administrator supprime les utilisateurs temporaires les plus anciens dans les bases de données d'utilisateurs iLO.

Informations de mappage de ports

Les informations de mappage de port sont disponibles en cliquant sur **Port Mapping Information** sur l'écran Device Bay Information.

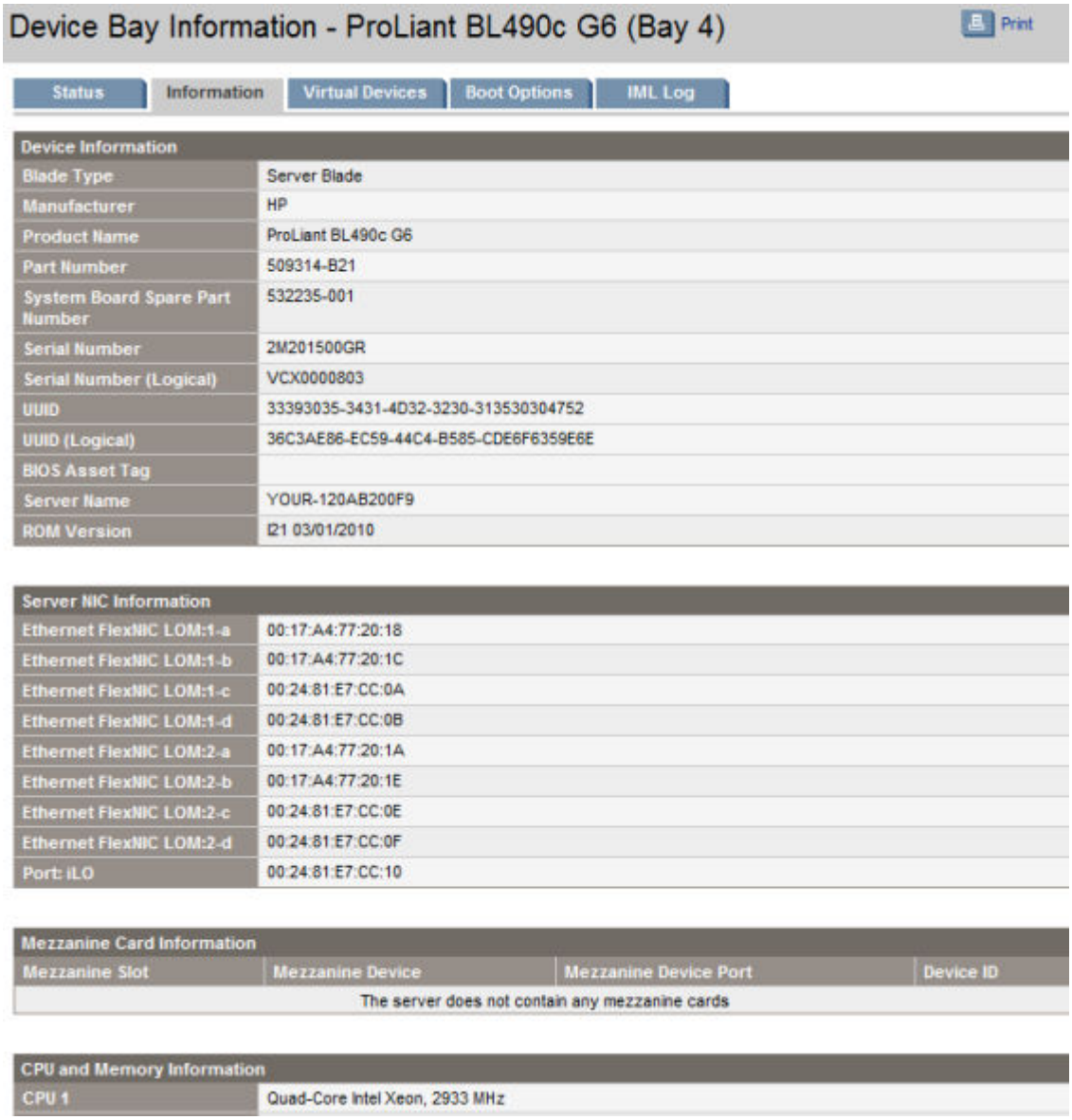
Pour plus d'informations, consultez la section « Mappage de ports » (Mappage de ports à la page 256).

Microprogramme

Il est possible d'accéder aux informations relatives aux microprogrammes des périphériques de la baie en cliquant sur **Firmware** (Microprogrammes).

Pour plus d'informations, consultez la section « Microprogramme » (Microprogrammes à la page 274).

Onglet Server Blade Information



Informations sur le périphérique

Rangée	Description
Blade Type (Type de lame)	Lame de serveur
Manufacturer (Fabricant)	Nom de la société qui a fabriqué la lame de serveur
Product Name (Nom du produit)	Nom descriptif courant de la lame de serveur
Part Number (Référence)	Numéro de référence utilisé pour commander une lame de serveur supplémentaire ou de remplacement de ce type
System Board Spare Part Number (Référence de rechange de carte mère)	Numéro de référence utilisé pour commander une carte mère supplémentaire ou de remplacement de ce type
Serial Number (Numéro de série)	Numéro de série usine statique de la lame de serveur
Serial Number (Logical) (Numéro de série (logique))	Numéro de série logique affecté à la lame de serveur

Rangée	Description
UUID	UUID attribué à la lame de serveur
UUID (logique)	UUID logique attribué à la lame de serveur
BIOS Asset Tag (Étiquette d'inventaire du BIOS)	Si configurée, étiquette d'inventaire de la lame de serveur installée
Server Name (Nom du serveur)	Si configuré via le BIOS, cela apparaît en tant que nom du serveur ProLiant. Pour les lames de serveur ProLiant ou Integrity dotées d'agents de système d'exploitation HP installés, il s'agit du nom hôte du serveur.*
ROM Version (Version de ROM)	Numéro de version de la ROM
Boot Mode (Mode Boot)	Mode démarrage pour la lame de serveur. Le mode Boot s'affiche uniquement si la lame de serveur prend en charge l'interface UEFI (Unified Extensible Firmware Interface). Les valeurs possibles sont Legacy, UEFI ou UEFI Optimized.
Secure Boot	État du mode Secure Boot du BIOS pour la lame de serveur. L'état Secure Boot est affiché uniquement si la lame de serveur est configurée en mode d'amorçage UEFI ou UEFI optimisé. Les valeurs possibles sont Enabled (Activé) et Disabled (Désactivé). Le mode Secure Boot empêche les utilisateurs (y compris l'administrateur) de modifier les paramètres par défaut du périphérique d'amorçage ou d'effectuer certaines opérations d'amorçage à partir de l'interface CLI ou de l'interface utilisateur du module Onboard Administrator. Toutes les modifications apportées aux paramètres d'amorçage doivent être établies dans le BIOS par l'administrateur. Les opérations d'amorçage peuvent être effectuées uniquement à partir du périphérique d'amorçage configuré dans le BIOS par l'administrateur. Le mode Secure Boot n'est pas indiqué pour des lames de serveur Gen8 et de générations antérieures. Pour plus d'informations sur l'utilisation du mode Secure Boot, consultez le *Manuel de l'utilisateur de HP UEFI System Utilities* sur le site Web HP (http://www.hp.com/go/ProLiantUEFI/docs).

* La console Web iLO permet de modifier le nom du serveur. Les serveurs iLO 2 ont une limite dans laquelle l'iLO alerte uniquement le module Onboard Administrator lorsque l'un des 28 premiers caractères du nom est modifié. Sinon, aucune notification n'est envoyée au module Onboard Administrator. Il en résulte que le nom du serveur indiqué dans le module Onboard Administrator peut être différent du nom du serveur iLO.

Informations de carte réseau de serveur

Rangée	Description
Ethernet FlexNIC LOM:(*x*)-(a-d)	Une carte réseau 10Gb compatible Flex-10 configurée dans Virtual Connect. Les quatre cartes réseau Flex sur le port *x* d'un LOM de serveur prenant en charge Flex-10 sont numérotées LOM:*x*-a, LOM:*x*-b, LOM:*x*-c, and LOM:*x*-d, où *x* est le port 1–4. Consultez le *Manuel de l'utilisateur de HP Virtual Connect c-Class BladeSystem* pour obtenir des informations détaillées sur la configuration de cartes réseau Flex-10.
Ethernet FlexNIC (NIC x) LOM: (*y*)-(a-d)	Une carte réseau 10Gb compatible Flex-10 configurée dans Virtual Connect, où x est une carte réseau 1–32. Les quatre cartes réseau Flex sur le port *y* d'un LOM de serveur prenant en charge Flex-10 sont numérotées LOM:*y*-a, LOM:*y*-b, LOM:*y*-c, and LOM:*y*-d, où *y* est le port 1–8. Consultez le

Rangée	Description
	Manuel de l'utilisateur de HP Virtual Connect c-Class BladeSystem pour obtenir des informations détaillées sur la configuration de cartes réseau Flex-10.
Port: NIC *x* (Port : carte réseau x)	Adresse MAC du port de cette carte réseau, où *x* est un port de carte réseau 1-4.
Port: iLO	Adresse MAC du port iLO de la lame de serveur dans ce logement de boîtier.
Port: iSCSI *x*	Adresse MAC du port de ce port iSCSI, où *x* est un port iSCSI 1-8.
Ethernet FCoE FlexFabric Adapter: (*y*)-(a-d)	Un adaptateur FCoE FlexFabric comprend 4 cartes réseau. Les quatre cartes réseau Flex sur le port *y* d'un LOM de serveur prenant en charge Flex-10 sont numérotées LOM:*y*-a, LOM:*y*-b, LOM:*y*-c, and LOM:*y*-d, où *y* est le port 1–8 LOM:*y*-b peut être utilisé pour configurer le trafic FCoE.
Ethernet iSCSI FlexFabric adapter: (*y*)-(a-d)	Un adaptateur iSCSI FlexFabric comprend 4 cartes réseau. Les quatre cartes réseau Flex sur le port *y* d'un LOM de serveur prenant en charge Flex-10 sont numérotées LOM:*y*-a, LOM:*y*-b, LOM:*y*-c, and LOM:*y*-d, où *y* est le port 1–8 LOM:*y*-b peut être utilisé pour configurer le trafic FCoE.

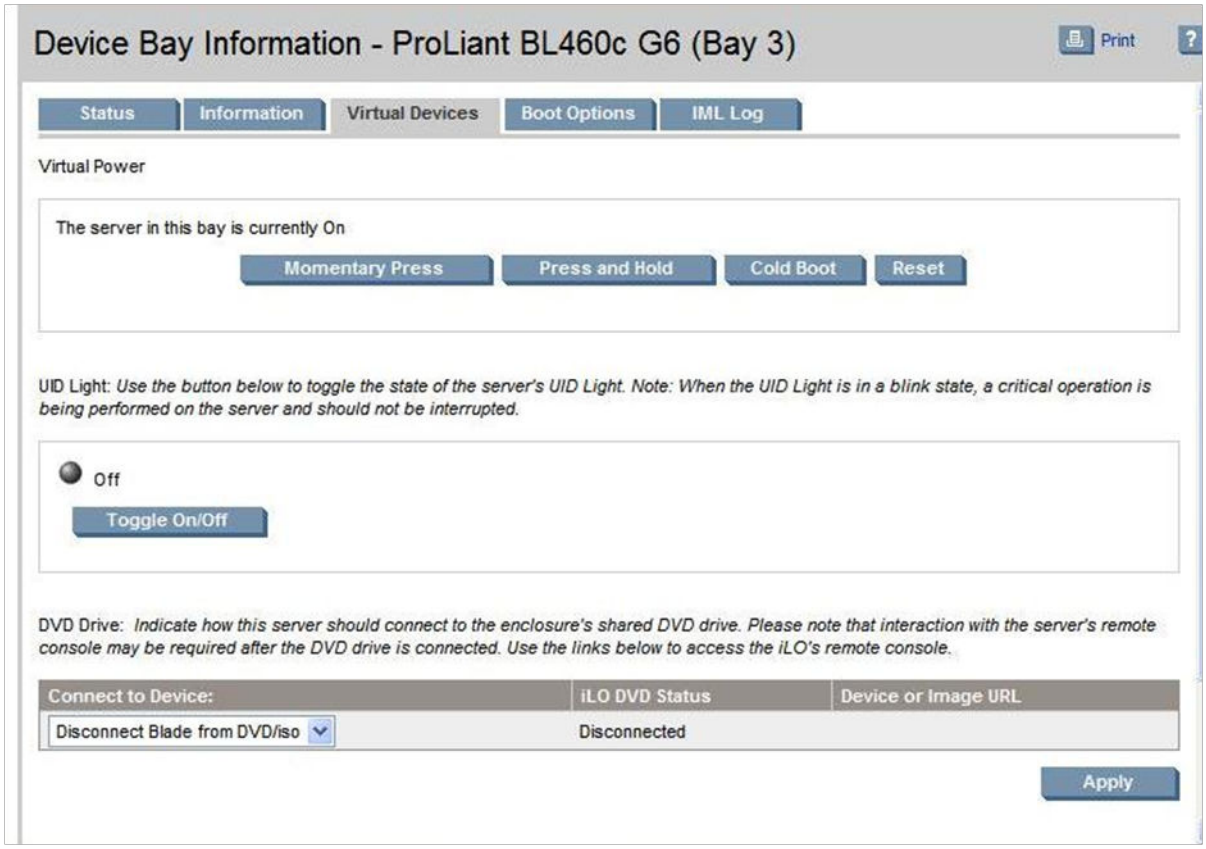
Informations de carte mezzanine

Colonne	Description
Mezzanine Slot (Connecteur mezzanine)	Connecteur physique dans lequel la carte mezzanine est située
Mezzanine Device (Périphérique mezzanine)	Nom commun ou de produit du périphérique mezzanine
Mezzanine Device Port (Port de périphérique mezzanine)	Port attribué au périphérique mezzanine
Device ID (ID du périphérique)	Adresse MAC du port de la baie d'interconnexion

Informations d'unité centrale et de mémoire

Rangée	Description
CPU 1 à CPU (x)	Type d'unité centrale ou Not present (Absent)
Memory	Taille de la mémoire

Onglet Server Blade Virtual Devices


Device Bay Information - ProLiant BL460c G6 (Bay 3)
Print
Status
Information
Virtual Devices
Boot Options
IML Log
Virtual Power
The server in this bay is currently On
Momentary Press
Press and Hold
Cold Boot
Reset
UID Light: Use the button below to toggle the state of the server's UID Light. Note: When the UID Light is in a blink state, a critical operation is being performed on the server and should not be interrupted.
Off
Toggle On/Off
DVD Drive: Indicate how this server should connect to the enclosure's shared DVD drive. Please note that interaction with the server's remote console may be required after the DVD drive is connected. Use the links below to access the iLO's remote console.
Connect to Device:
iLO DVD Status
Device or Image URL
Disconnect Blade from DVD/iso
Disconnected
Apply

Virtual Power

Bouton	Description
Momentary Press (Pression momentanée)	Ce bouton réplique une pression momentanée physique du bouton d'alimentation sur la lame de serveur. Un clic sur ce bouton met sous ou hors tension la lame de serveur de manière ordonnée.
Press and Hold (Appuyer et maintenir enfoncé)	Ce bouton réplique une pression physique et un maintien enfoncé du bouton d'alimentation sur la lame de serveur. Un clic sur ce bouton force la mise hors tension de la lame de serveur sans mise hors tension préalable du système d'exploitation. Cette option n'est pas disponible lorsque la lame de serveur est hors tension.
Cold Boot (Démarrage à froid)	Un clic sur ce bouton supprime immédiatement l'alimentation du système. Cette option n'est pas disponible lorsque la lame de serveur est hors tension.
Reset (Réinitialiser)	Un clic sur ce bouton effectue une réinitialisation du système. Cette option n'est pas disponible lorsque la lame de serveur est hors tension.

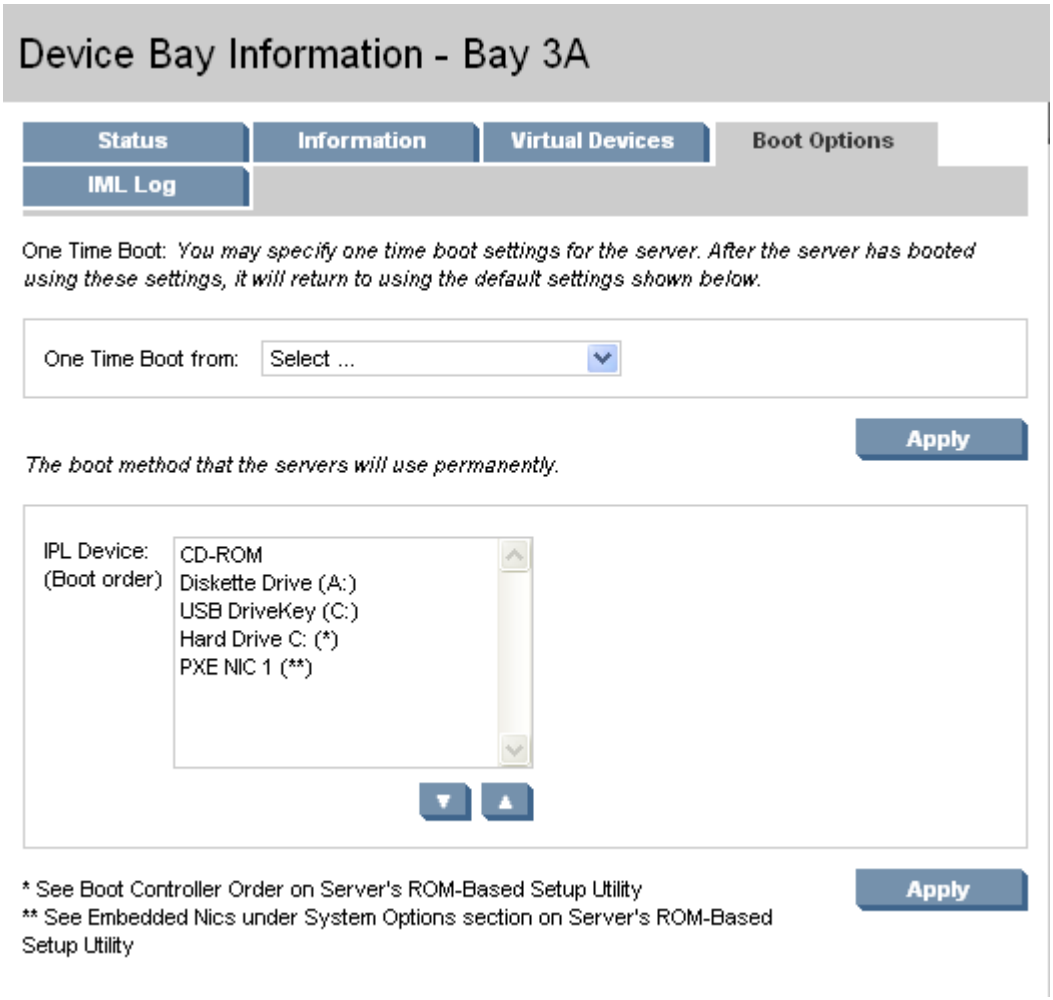
UID Light (Voyant UID)

Pour vous aider à identifier une lame de serveur spécifique, cliquez sur **Toggle On/Off** pour allumer (bleu) ou éteindre (gris) le voyant d'UID de la lame de serveur.

DVD Drive (Lecteur de CD/DVD-ROM)

Colonne	Description
Connect to Device (Se connecter au périphérique)	Ce menu permet de connecter ou déconnecter le lecteur de DVD partagé en sélectionnant **Connect to Enclosure DVD** (Connecter au DVD du boîtier) ou **Disconnect DVD Hardware** (Déconnecter matériel DVD).
iLO DVD Status (État de DVD iLO)	Ce champ indique si la lame de serveur dispose d'une connexion Virtual Media. Les valeurs possibles sont Connected (Connecté) ou Disconnected (Déconnecté). Un état Incompatible Firmware (Microprogramme incompatible) indique que la fonctionnalité DVD n'est pas prise en charge avec le microprogramme iLO installé sur le périphérique.
Device or Image URL (URL d'image ou périphérique)	Ce champ affiche la connexion Virtual Media actuelle de la lame. Les valeurs possibles sont : • Virtual Media Applet is connected • Feature not supported on Integrity iLO version x.xx • SSH is disabled on this blade's iLO processor • Upgrade ProLiant iLO version x.xx to 1.30 or higher • Enclosure DVD • Tray Open or No Media • URL to USB key ISO image file • iLO has no IP address

Onglet Boot Options


Device Bay Information - Bay 3A
Status
Information
Virtual Devices
Boot Options
IML Log
One Time Boot: You may specify one time boot settings for the server. After the server has booted using these settings, it will return to using the default settings shown below.
One Time Boot from:
Select ...
Apply
The boot method that the servers will use permanently.
IPL Device:
(Boot order)
CD-ROM
Diskette Drive (A:)
USB DriveKey (C:)
Hard Drive C: (*)
PXE NIC 1 (**)
Apply
* See Boot Controller Order on Server's ROM-Based Setup Utility
** See Embedded Nics under System Options section on Server's ROM-Based Setup Utility

One Time Boot from selections (Démarrage ponctuel sur sélections)

Si vous spécifiez des paramètres de démarrage unique, ceux-ci sont valides uniquement pour le prochain réamorçage de la lame de serveur. Une fois que l'amorçage est terminé, la lame de serveur utilise les paramètres par défaut (ordre d'amorçage de périphérique d'IPL) pour les redémarrages suivants.

Option	Description
Select (Sélectionner)	Option par défaut lors du premier affichage ou avant l'apport de toute modification.
No one time Boot (Pas de démarrage unique)	Force la lame de serveur à effacer les paramètres de démarrage unique.
Diskette Drive (A:) (Lecteur de disquette (A:))	Force la lame de serveur à redémarrer à partir du lecteur de disquette. Vérifiez que le lecteur de disquette est connecté à la lame de serveur avant de sélectionner cette option.
CD-ROM	Force la lame de serveur à redémarrer à partir du lecteur de CD-ROM. Vérifiez que le lecteur de CD-ROM est connecté à la lame de serveur avant de sélectionner cette option.
Hard Drive C: (Disque dur C:)	Force la lame de serveur à redémarrer à partir du disque dur.

Option	Description
RBSU	Force la lame de serveur à démarrer sur l'outil ROM-Based Setup Utility.
PXE NIC	Force la lame de serveur à démarrer à partir de la carte réseau PXE.
USB	Force la lame de serveur à démarrer à partir de la clé USB.
Embedded UEFI Shell (Shell UEFI intégré)	Force la lame de serveur à démarrer à partir du shell UEFI intégré. Cette option n'est pas disponible pour une lame non compatible UEFI.
UEFI Target (cible UEFI)	Force la lame de serveur à démarrer à partir du périphérique cible UEFI. Cette option n'est pas disponible pour un serveur non compatible UEFI ou pour un serveur compatible UEFI en mode d'amorçage BIOS hérité.

Pour enregistrer les paramètres, cliquez sur **Apply** (Appliquer).

Si Secure Boot est configuré sur la lame de serveur, l'option One Time Boot ne peut pas être sélectionnée. Cette option est grisée. Le mode Secure Boot empêche les utilisateurs (y compris l'administrateur) d'effectuer cette opération à partir de l'interface CLI ou de l'interface utilisateur du module Onboard Administrator. Les opérations d'amorçage peuvent être effectuées uniquement à partir du périphérique d'amorçage configuré dans le BIOS par l'administrateur.

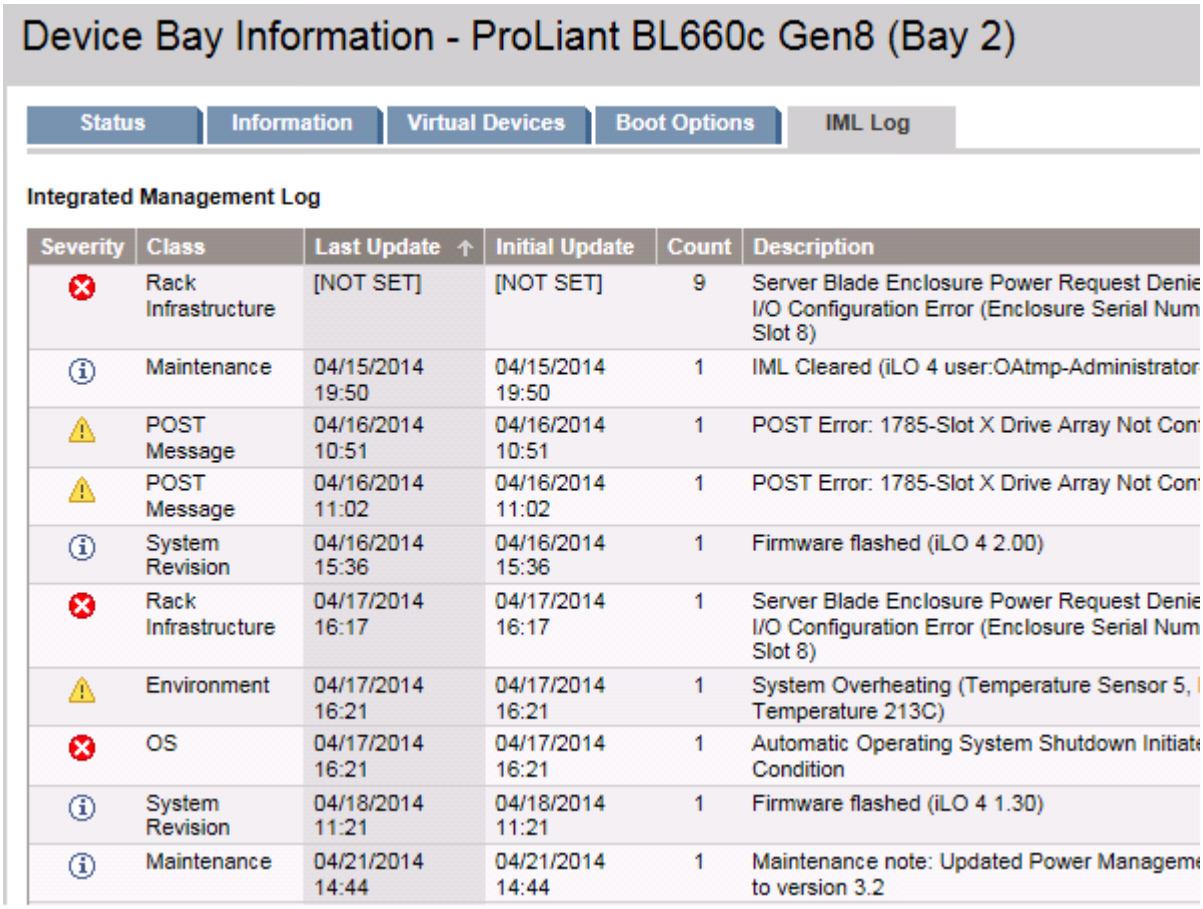
Standard Boot Order (IPL) (Ordre d'amorçage standard (IPL))

Pour spécifier un ordre de démarrage standard, sélectionnez un périphérique dans la liste définissant l'ordre de démarrage et utilisez les flèches haut et bas pour le déplacer à votre convenance. Continuez de la sorte jusqu'à ce que les périphériques soient classés dans l'ordre d'utilisation voulu. Le RBSU peut également être utilisé pour définir l'ordre de démarrage standard. Tous les démarrages, sauf pour l'option One Time Boot (Démarrage ponctuel), utilisent l'ordre de démarrage standard défini.

Pour enregistrer les paramètres, cliquez sur **Apply** (Appliquer).

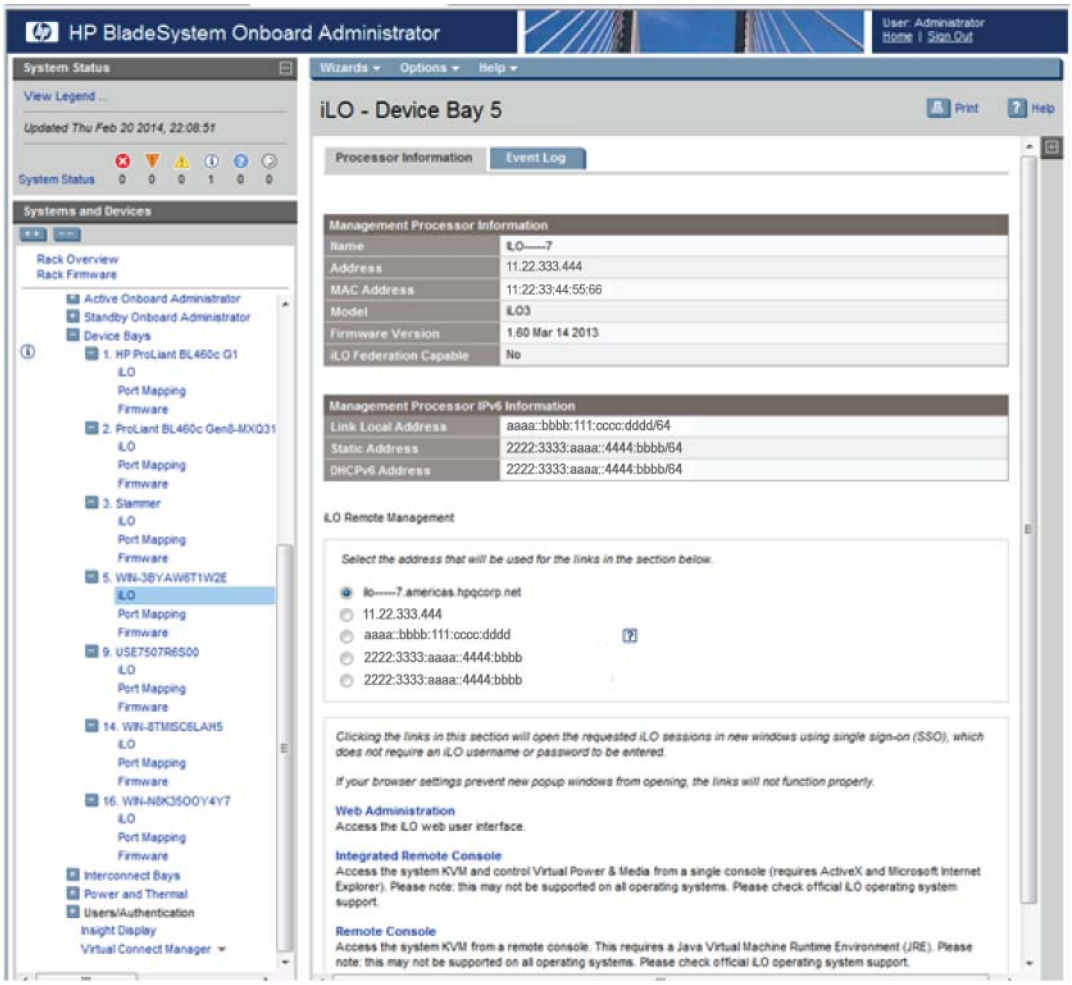
Si Secure Boot est configuré sur la lame de serveur, les périphériques IPL ne peuvent pas être sélectionnés. La liste des périphériques apparaît en grisé. Le mode Secure Boot empêche les utilisateurs (y compris l'administrateur) d'effectuer cette opération à partir de l'interface CLI ou de l'interface utilisateur du module Onboard Administrator. Les opérations d'amorçage peuvent être effectuées uniquement à partir du périphérique d'amorçage configuré dans le BIOS par l'administrateur.

Onglet IML Log



L'onglet IML Log (Journal de maintenance intégré) présente les informations enregistrées dans le journal de maintenance (IML) de la lame de serveur. Les informations contenues dans le journal peuvent être des données pour information, d'avertissement ou critiques. Les colonnes Last Update (Dernière mise à jour) et Initial Update (Mise à jour initiale) affichent des dates et la colonne Count (Décompte) indique le nombre de fois que l'entrée a été consignée. La colonne Description affiche la description détaillée de l'entrée.

Écran iLO



Les informations présentées sur cet écran incluent des onglets concernant les informations de processeur, les informations de processeur d'IPv6 et le journal des événements. Pour afficher les vues avant et arrière de la baie de périphérique, cliquez sur la **flèche gauche** située dans le coin supérieur droit de l'écran.

Onglet Processor Information

Rangée	Description
Name	Nom DNS du processeur iLO.
Address (Adresse)	Adresse IP du processeur iLO.
Adresse MAC	Adresse MAC du processeur iLO.
Modèle	Descripteur courant du processeur iLO.
Firmware Version (Version du microprogramme)	Version installée du microprogramme du processeur iLO.
VLAN ID (Name) (ID VLAN [Nom])	Numéro d'ID VLAN et nom VLAN de la baie de périphérique lorsque le réseau VLAN est activé.
Compatible iLO Federation	Indique si la lame de serveur est compatible avec iLO Federation.

Rangée	Description
	Cela indique uniquement si iLO est capable d'être configuré pour participer dans iLO Federation. Cela n'indique pas si iLO est actuellement configuré pour une participation effective dans iLO Federation. Pour activer complètement iLO Federation, la prise en charge de Enclosure iLO Federation doit être activée sur le module Onboard Administrator (pour plus d'informations, voir la page Network Access) et chaque système iLO doit disposer du microprogramme approprié et être configuré pour prendre en charge iLO Federation (pour plus d'informations, voir le *Manuel de l'utilisateur de HP iLO 4* sur le site Web HP (http://www.hp.com/go/ilo/docs)).

Informations IPv6 du processeur

Rangée	Description
Link Local Address (Adresse locale du lien)	Adresse IPv6 locale du lien du processeur iLO
Static Address (Adresse statique)	Adresse IPv6 statique du processeur iLO
EBIPA Address (Adresse EBIPA)	Adresse IPv6 EBIPA du processeur iLO
Adresse DHCPv6	Adresse IPv6 DHCP du processeur iLO
Adresse SLAAC	Adresse IPv6 SLAAC du processeur iLO

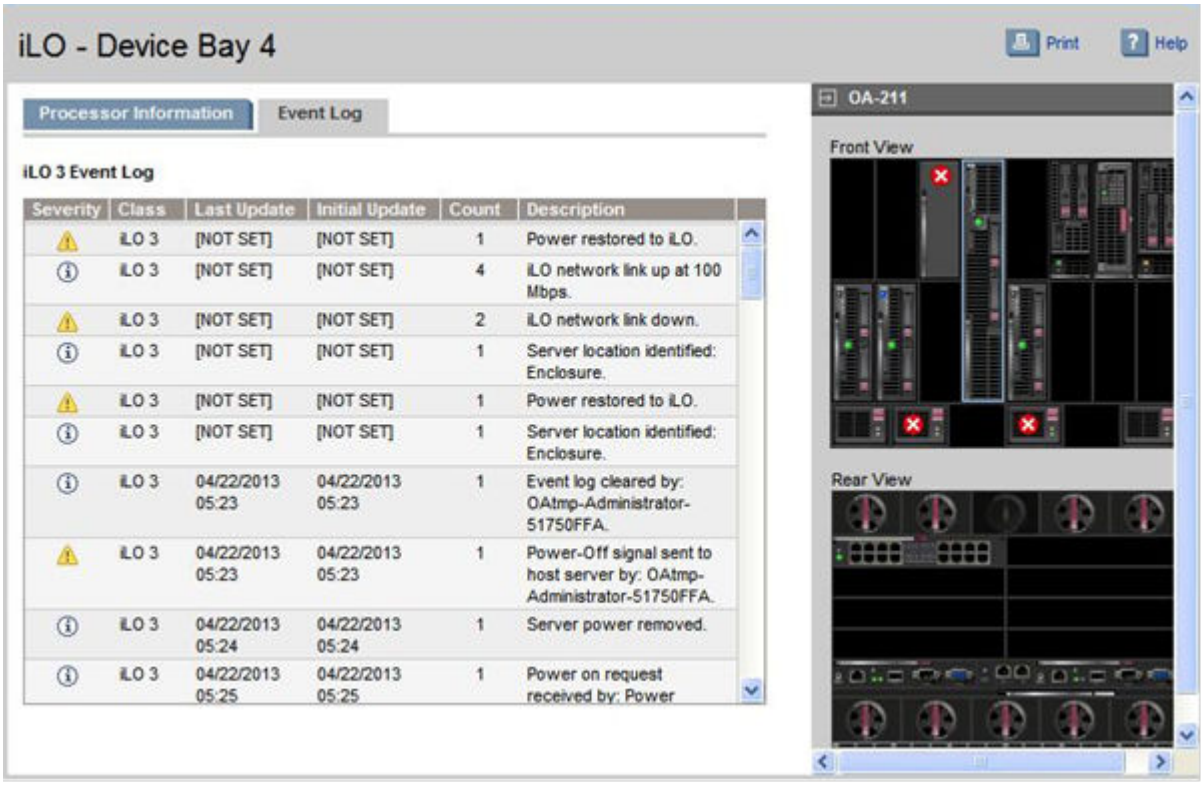
Supervision distante iLO

Cette section fournit des liens vers les sessions iLO demandées.

Lorsque le protocole IPv6 est activé, ou que la prise en charge du lien FQDN est activée, une zone de groupe d'adresses IP s'affiche. Cette zone de groupe permet de sélectionner l'adresse IP à utiliser pour les liens d'accès aux sessions iLO. Si la prise en charge du lien FQDN est activée et que certaines exigences de configuration DNS sont remplies, une adresse basée sur le nom de domaine complet est la sélection par défaut. Pour plus d'informations sur l'activation de la prise en charge du lien FQDN, consultez la page « Accès réseau ».

Si vous essayez d'utiliser une fonction qui nécessite la prise en charge des fenêtres contextuelles et que la fonction ne fonctionne pas correctement, assurez-vous que les paramètres du navigateur n'empêchent pas l'ouverture des fenêtres contextuelles. Pour obtenir de l'aide sur la désactivation des bloqueurs de fenêtres contextuelles, consultez les fichiers d'aide de votre navigateur.

Onglet iLO Event Log


iLO - Device Bay 4
Print
Help
Processor Information
Event Log
iLO 3 Event Log
Severity
Class
Last Update
Initial Update
Count
Description
iLO 3 [NOT SET] [NOT SET] 1 Power restored to iLO.
iLO 3 [NOT SET] [NOT SET] 4 iLO network link up at 100 Mbps.
iLO 3 [NOT SET] [NOT SET] 2 iLO network link down.
iLO 3 [NOT SET] [NOT SET] 1 Server location identified: Enclosure.
iLO 3 [NOT SET] [NOT SET] 1 Power restored to iLO.
iLO 3 [NOT SET] [NOT SET] 1 Server location identified: Enclosure.
iLO 3 04/22/2013 05:23 04/22/2013 05:23 1 Event log cleared by: OAtmp-Administrator-51750FFA.
iLO 3 04/22/2013 05:23 04/22/2013 05:23 1 Power-Off signal sent to host server by: OAtmp-Administrator-51750FFA.
iLO 3 04/22/2013 05:24 04/22/2013 05:24 1 Server power removed.
iLO 3 04/22/2013 05:25 04/22/2013 05:25 1 Power on request received by: Power
OA-211
Front View
Rear View

Cet onglet affiche les informations du journal des événements iLO provenant du module iLO. Celui-ci ne peut pas être modifié depuis l'interface graphique du module Onboard Administrator. Consultez la documentation iLO pour obtenir des informations détaillées sur le journal des événements iLO.

Mappage de ports

L'écran Port Mapping s'affiche lorsque vous cliquez sur **Port Mapping Information** dans l'écranDevice Bay Information.

Les deux écrans suivants affichent des exemples des onglets **Graphical View** (Vue graphique) et **Table View** (Vue de tableau) de l'écran Port Mapping.

Vue graphique

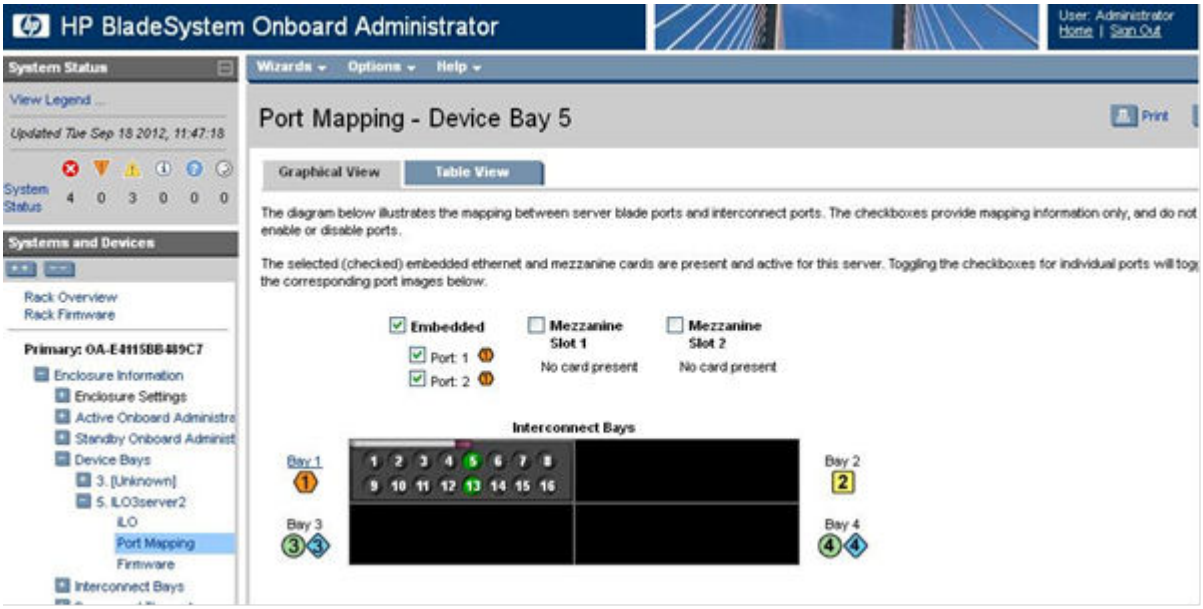
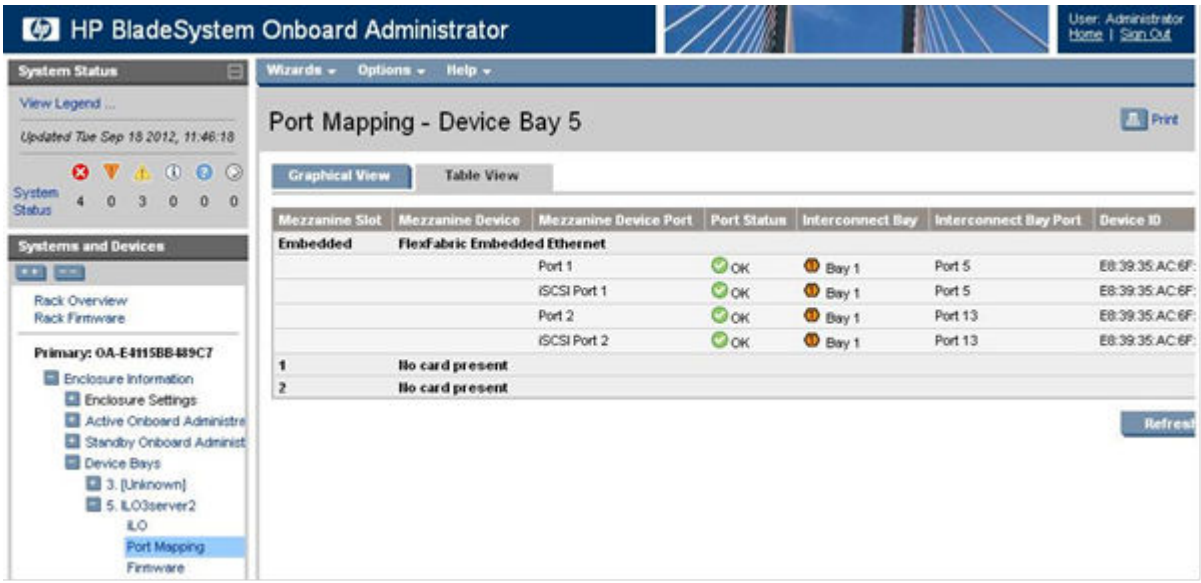


Table View

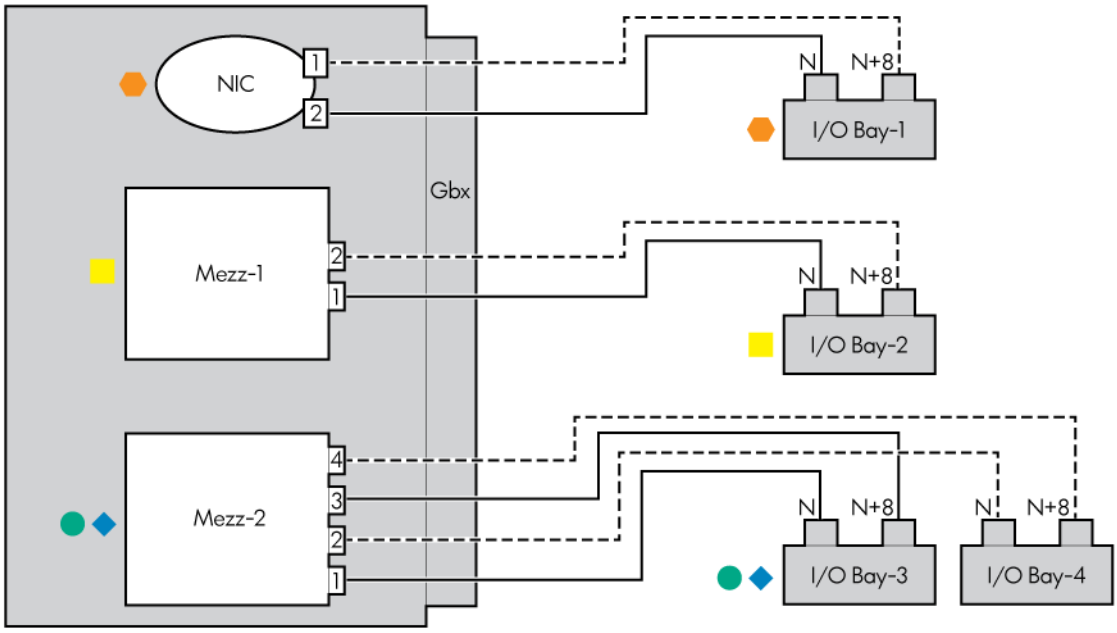


Pour plus d'informations, consultez les sections suivantes dans ce document. En outre, reportez-vous à la dernière documentation des boîtiers c3000 et c7000 dans la Bibliothèque d'informations de HP BladeSystem (http://www.hp.com/support/BladeSystem/docs).

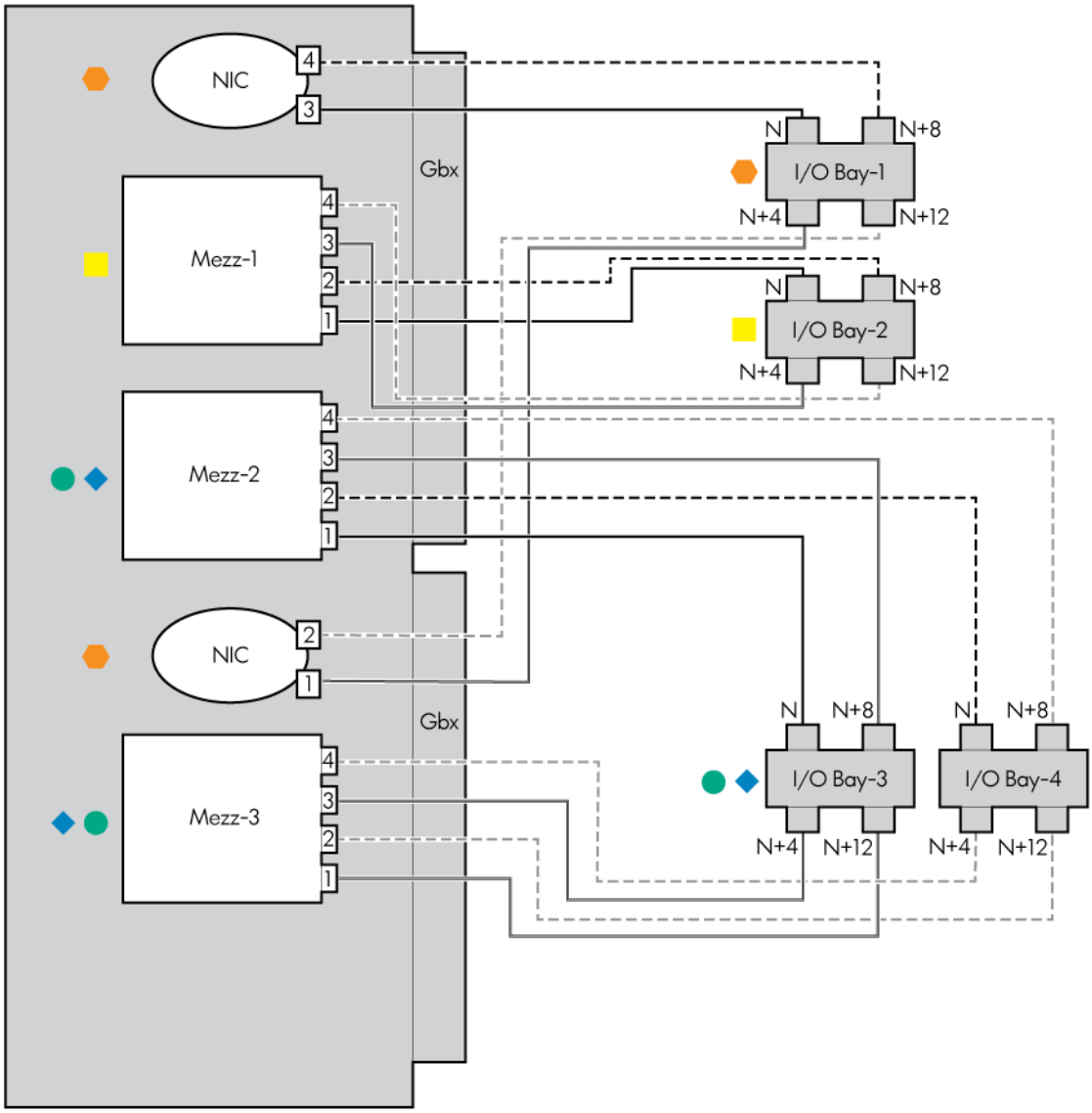
- « Vue graphique de mappage de ports de baie de périphérique pour boîtier c3000 » (Vue graphique de mappage de ports de baie de périphérique pour boîtier c3000 à la page 258)
- « Tableau de mappage de ports de baie de périphérique pour boîtier c3000 » (Tableau de mappage de ports de baie de périphérique pour boîtier c3000 à la page 262)
- « Vue graphique de mappage de ports de baie de périphérique pour boîtier c7000 » (Vue graphique de mappage de ports de baie de périphérique pour boîtier c7000 à la page 266)
- « Tableau de mappage de ports de baie de périphérique pour boîtier c7000 » (Tableau de mappage de ports de baie de périphérique pour boîtier c7000 à la page 271)

Vue graphique de mappage de ports de baie de périphérique pour boîtier c3000

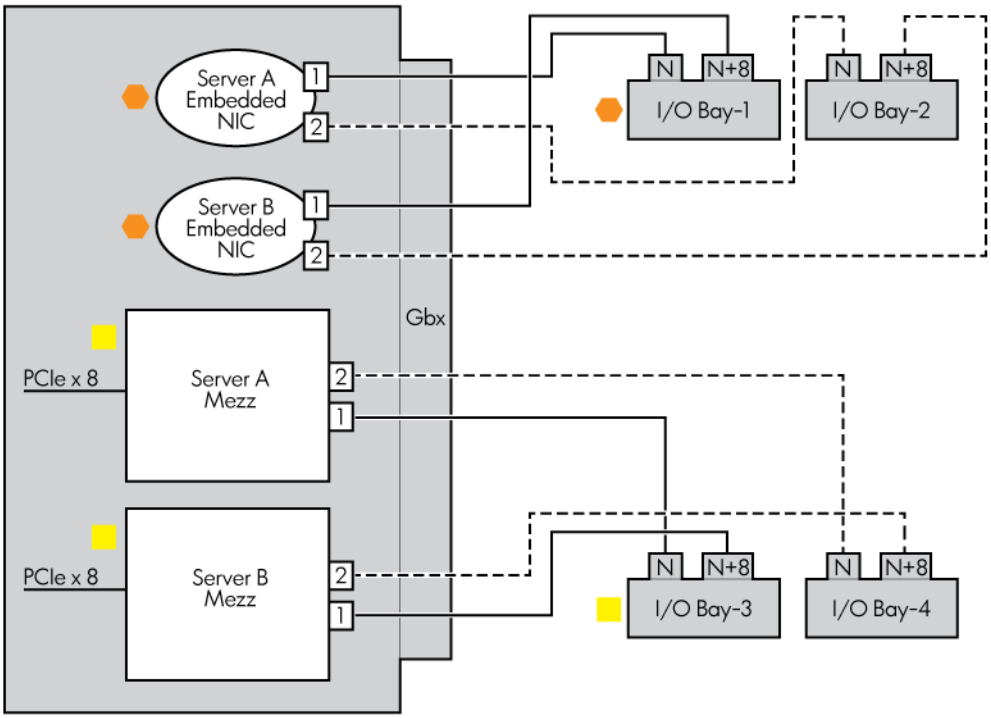
Lames de serveur demi-hauteur, simple largeur (par exemple, des serveurs HP ProLiant BL260c, BL280c, BL420c, BL460c, BL465c, BL490c, BL495c et WS460c)



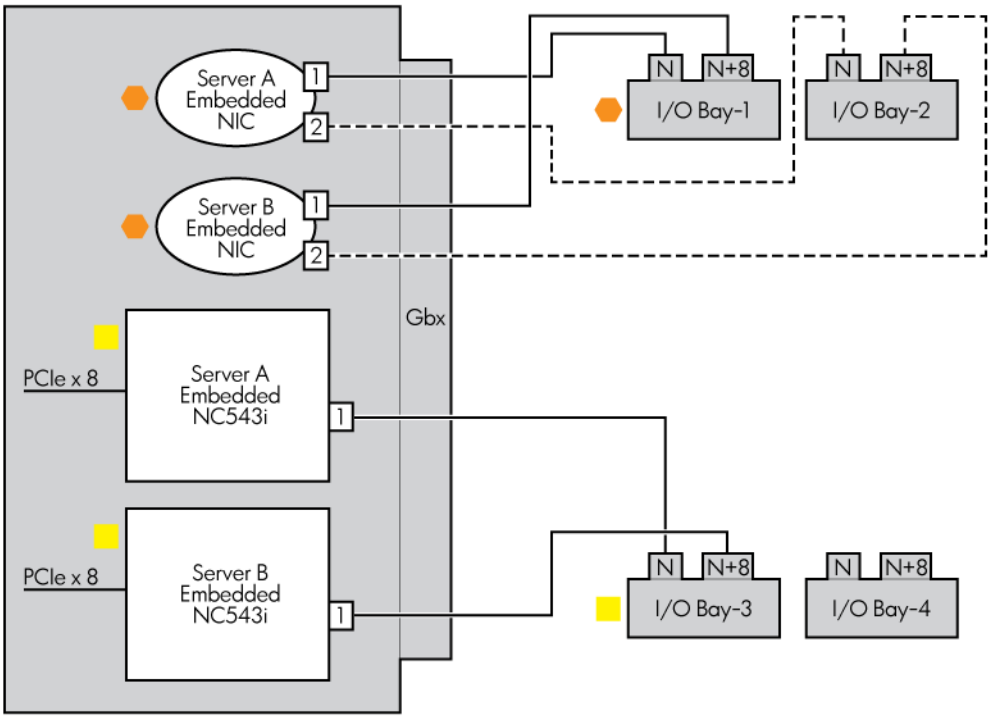
Lame de serveur pleine hauteur, simple largeur (telles que HP ProLiant BL680c (G1), BL680c Gen5, et BL480c, BL620c, BL660c et BL685c)



Lames de serveur demi-hauteur, double densité, telles que HP ProLiant BL2x220c (G1)–G6

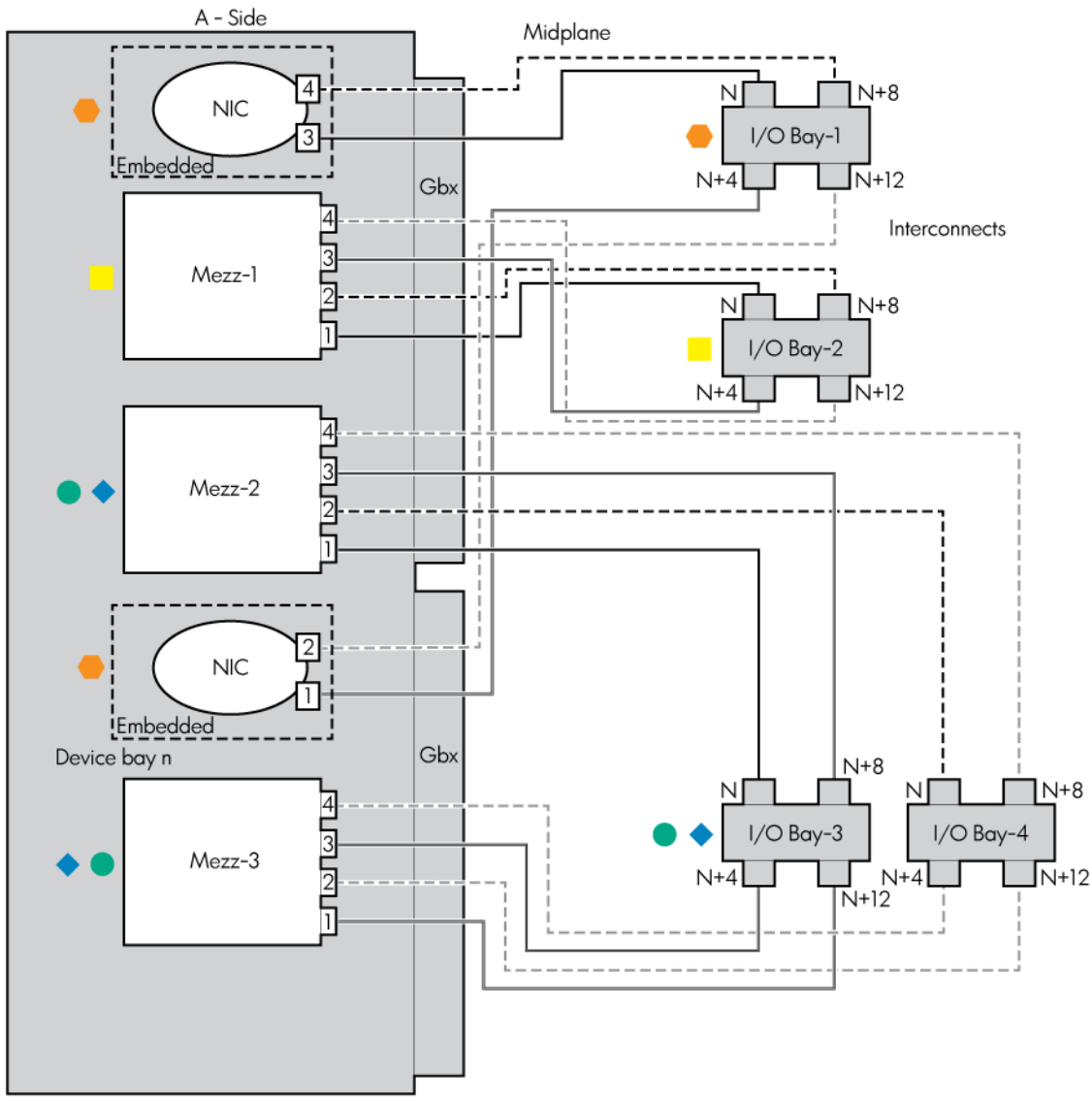


Lames de serveur demi-hauteur, double densité, telles que HP ProLiant BL2x220c G7



Lames de serveur pleine hauteur, double largeur telles que HP ProLiant BL680c G7

Côté A


A - Side
Midplane
NIC
4
3
Embedded
Gbx
N
N+8
I/O Bay-1
N+4
N+12
Interconnects
Mezz-1
4
3
2
1
N
N+8
I/O Bay-2
N+4
N+12
Mezz-2
4
3
2
1
NIC
2
1
Embedded
Device bay n
Gbx
N+8
N
I/O Bay-3
N+4
N+12
N
N+8
I/O Bay-4
N+4
N+12
Mezz-3
4
3
2
1

Côté B

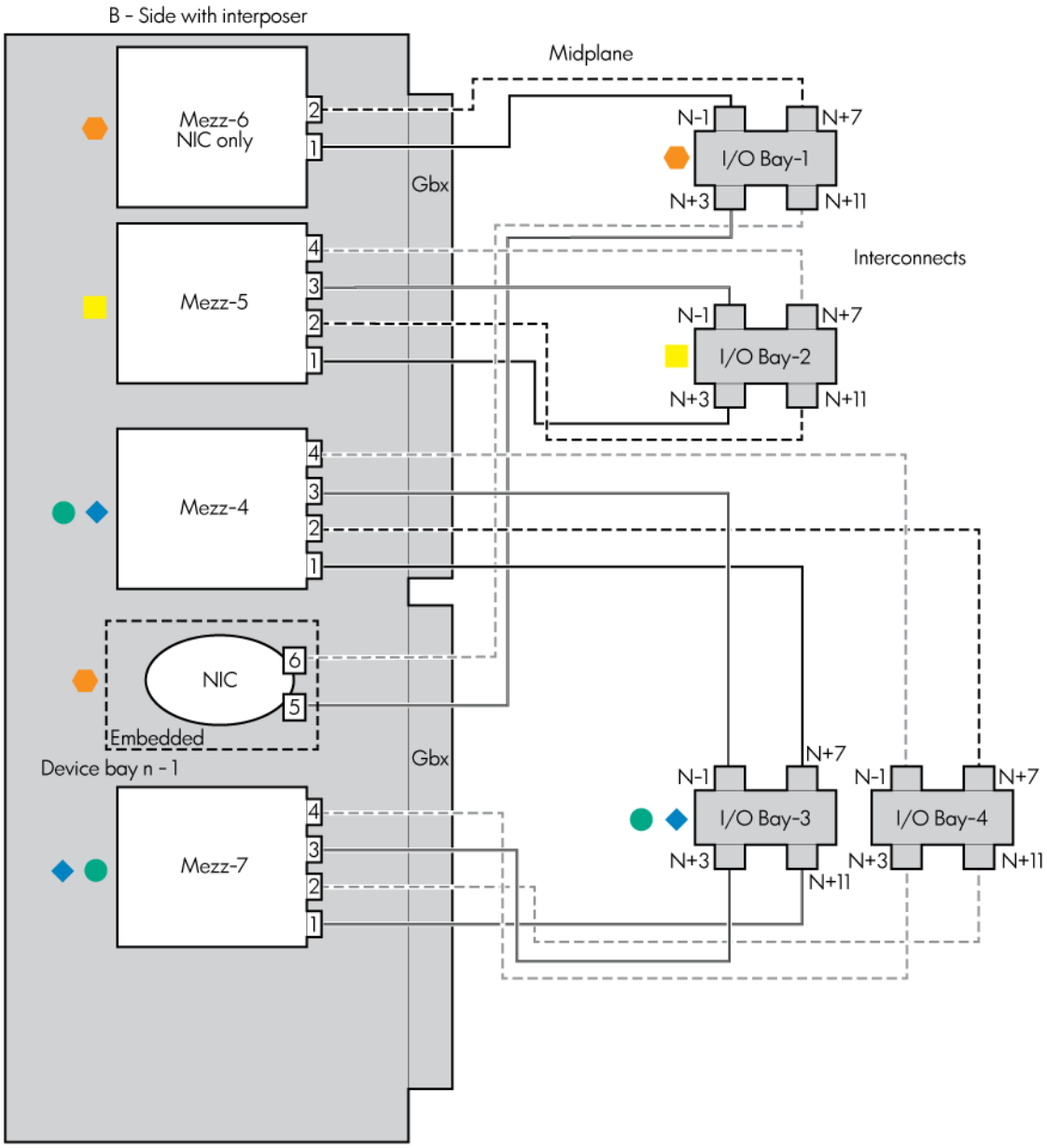


Tableau de mappage de ports de baie de périphérique pour boîtier c3000

Les lames de serveur sont reliées aux baies d'interconnexion de la manière suivante : Le terme 1x, 2x ou 4x désigne le nombre de voies d'interconnexion par port fournies par le contrôleur. Si aucun périphérique n'est présent, la case à cocher est désactivée et le port ne peut pas être affiché.

- Des exemples de ports 1x incluent 1GB Ethernet (1 GbE), 10GB Ethernet (10 GbE) et tous les périphériques Fibre Channel.
- Des exemples de ports 2x incluent 20GB Ethernet (20 GbE) et tous les périphériques SCSI (SAS) connectés en série.
- Des exemples de ports 4x incluent tous les périphériques InfiniBand.
- Les tableaux suivants font référence aux ports Ethernet en tant que cartes réseau.

REMARQUE : Les cartes mezzanine des ports 1x et 2x assurent l'interface avec les modules d'interconnexion simple largeur. Les cartes mezzanine à 4x ports s'interfacent avec les modules d'interconnexion à deux niveaux.

Lames de serveur demi-hauteur, simple largeur

Le tableau suivant répertorie le mappage de ports pour des lames de serveur demi-hauteur installées dans une baie de périphérique demi-hauteur N (1-8) de boîtier c3000. Des exemples de lames de serveur demi-hauteur comprennent les serveurs HP ProLiant BL260c, BL280c, BL420c, BL460c, BL465c, BL490c, BL495c et WS460c.

Connexion	Numéro de port	Connexion à baie d'interconnexion/port	Remarques
Carte réseau *	Carte réseau intégrée 1 (Port: 1) Carte réseau intégrée 2 (Port: 2)	1/Port N 1/Port N+8	Un module d'interconnexion Ethernet simple largeur
Connecteur mezzanine 1 — cartes 1x ou 2x (les cartes 4x ne sont pas prises en charge par ce connecteur)	Port 1 1x/2x Port 2 1x/2x	2/Port N 2/Port N+8	• Un module d'interconnexion simple largeur • Seuls deux ports seront connectés. • Quatre cartes de ports connectent uniquement les deux premiers ports.
Connecteur mezzanine 2 — cartes 1x ou 2x	Port 1 1x/2x Port 2 1x/2x Port 3 1x/2x Port 4 1x/2x	3/Port N 4/Port N 3/Port N+8 4/Port N+8	Un ou deux modules d'interconnexion de largeur simple
Connecteur mezzanine 2 — cartes 4x	Port 1 4x Port 2 4x	3/Port N 3/Port N+8	Un module d'interconnexion double largeur

* Les lames de serveur G7 et de générations précédentes incluent les ports Ethernet intégrés sur la carte mère. Avec les lames de serveur Gen8 et de générations ultérieures, les ports Ethernet sont situés sur une carte sélectionnable par l'utilisateur appelée une carte (adaptateur) FlexibleLOM. Les ports de carte FlexibleLOM et les ports de carte réseau intégré ont le même mappage.

Lames de serveur pleine hauteur, simple largeur

Le tableau suivant répertorie le mappage de ports pour des lames de serveur pleine hauteur, simple largeur installées dans une baie de périphérique pleine hauteur N (1-4) de boîtier c3000. Des exemples de ces lames de serveur pleine hauteur comprennent les serveurs HP ProLiant BL680c (G1), BL680c Gen5, et BL480c, BL620c, BL660c et BL685c.

Connexion	Numéro de port	Connexion à baie d'interconnexion/port	Remarques
Carte réseau*	Carte réseau intégrée 1 (Port: 1) Carte réseau intégrée 2 (Port: 2)	1/Port N+4 1/Port N+12 1/Port N 1/Port N+8	Un module d'interconnexion Ethernet simple largeur

Connexion	Numéro de port	Connexion à baie d'interconnexion/port	Remarques
	Carte réseau intégrée 3 (Port: 3)		
	Carte réseau intégrée 4 (Port: 4)		
Connecteur mezzanine 1 — cartes 1x ou 2x (les cartes 4x ne sont pas prises en charge par ce connecteur)	Port 1 1x/2x	2/Port N	Un module d'interconnexion simple largeur
	Port 2 1x/2x	2/Port N	
	Port 3 1x/2x	2/Port N+4	
	Port 4 1x/2x	2/Port N+12	
Connecteur mezzanine 2 — cartes 1x ou 2x	Port 1 1x/2x	3/Port N	Un ou deux modules d'interconnexion de largeur simple
	Port 2 1x/2x	4/Port N	
	Port 3 1x/2x	3/Port N+8	
	Port 4 1x/2x	4/Port N+8	
Connecteur mezzanine 2 — cartes 4x	Port 1 4x	3/Port N	Un module d'interconnexion double largeur
	Port 2 4x	3/Port N+8	
Connecteur mezzanine 3 — cartes 1x ou 2x	Port 1 1x/2x	3/Port N+12	Un ou deux modules d'interconnexion de largeur simple
	Port 2 1x/2x	4/Port N+12	
	Port 3 1x/2x	3/Port N+4	
	Port 4 1x/2x	4/Port N+4	
Connecteur mezzanine 3 — cartes 4x	Port 1 4x	3/Port N+12	Un module d'interconnexion double largeur
	Port 2 4x	3/Port N+4	

* Les lames de serveur G7 et de générations précédentes incluent les ports Ethernet intégrés sur la carte mère. Avec les lames de serveur Gen8 et de générations ultérieures, les ports Ethernet sont situés sur une carte sélectionnable par l'utilisateur appelée une carte (adaptateur) FlexibleLOM. Les ports de carte FlexibleLOM et les ports de carte réseau intégré ont le même mappage.

Lames de serveur demi-hauteur, double densité, telles que les serveurs HP ProLiant BL2x220 (G1) - G6

Le tableau suivant répertorie les configurations disponibles pour des lames de serveur double densité installées dans une baie de périphérique demi-hauteur N (1-8) de boîtier c3000. Des exemples de ces lames de serveur double densité comprennent les serveurs HP ProLiant BL2x220c (G1) - G6.

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
Carte réseau intégrée de serveur A	Carte réseau intégrée 1 (Port: 1)	1/Port N
	Carte réseau intégrée 2 (Port: 2)	2/Port N
Carte mezzanine de serveur A	Port 1	3/Port N
	Port 2	4/Port N
Carte réseau intégrée de serveur B	Carte réseau intégrée 1 (Port: 1)	1/Port N+8
	Carte réseau intégrée 2 (Port: 2)	2/Port N+8
Carte mezzanine de serveur B	Port 1	3/Port N+8

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
	Port 2	4/Port N+8

Lames de serveur demi-hauteur, double densité, telles que HP ProLiant BL2x220c G7

Le tableau suivant répertorie les configurations disponibles pour des périphériques double densité tels que les modèles HP ProLiant BL2x220c G7 installés dans une baie de périphérique demi-hauteur N (1-8) de boîtier c3000.

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
Carte réseau intégrée de serveur A	Carte réseau intégrée 1 (Port: 1)	1/Port N
	Carte réseau intégrée 2 (Port: 2)	2/Port N
Carte NC543i* intégrée de serveur A	Port 1	3/Port N
Carte réseau intégrée de serveur B	Carte réseau intégrée 1 (Port: 1)	1/Port N+8
	Carte réseau intégrée 2 (Port: 2)	2/Port N+8
Carte NC543i* intégrée de serveur B	Port 1	3/Port N+8

***** La carte NC543i intégrée de lame de serveur HP ProLiant BL2x220c G7 est automatiquement configurée par le module Onboard Administrator pour Ethernet, si un module d'interconnexion Ethernet est installé dans la baie 3, ou pour InfiniBand si une interconnexion InfiniBand double largeur est installée dans la baie 3. Pour changer la configuration NC543i d'un type à un autre, mettez hors tension toutes les lames de serveur HP ProLiant BL2x220c G7 et remplacez le module d'interconnexion par l'autre type. Redémarrez le module Onboard Administrator actif ou réinstallez toutes les lames de serveur HP ProLiant BL2x220c G7 : le module Onboard Administrator reconfigure toutes les cartes NC543i intégrées pour le nouveau type d'interconnexion.

Lame d'extension E/S AMC Telco

Le tableau suivant répertorie les configurations disponibles pour des périphériques AMC Telco installés dans une baie de périphérique demi-hauteur N (1-8) de boîtier c3000.

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
Lame AMC intégrée (1)	Port 1	1/Port N
	Port 3	2/Port N
Lame AMC intégrée (2)	Port 5	3/Port N
	Port 7	4/Port N

Lames de serveur pleine hauteur, double largeur telles que HP ProLiant BL680c G7

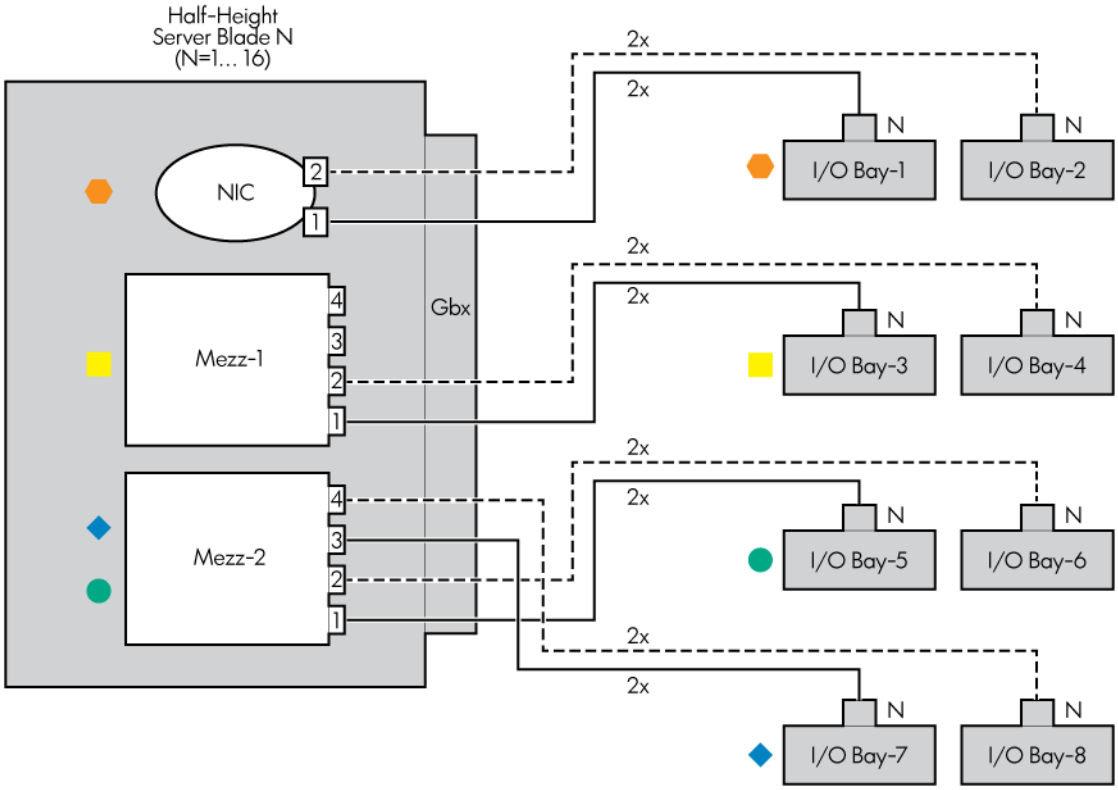
Le tableau suivant répertorie les configurations disponibles pour des lames de serveur pleine hauteur, double largeur, telles que les serveurs HP ProLiant BL680c G7, installées dans une baie de périphérique c3000 N (2 ou 4).

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
Carte réseau intégrée côté A	Carte réseau 1	1/Port N+4
	Carte réseau 2	1/Port N+12

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
	Carte réseau 3	1/Port N
	Carte réseau 4	1/Port N+8
Carte réseau intégrée côté B	Carte réseau 5	1/Port N+3
	Carte réseau 6	1/Port N+11
Mezzanine 1 côté A	Port 1	2/Port N
	Port 2	2/Port N+8
	Port 3	2/Port N+4
	Port 4	2/Port N+12
Mezzanine 2 côté A	Port 1	3/Port N
	Port 2	4/Port N
	Port 3	3/Port N+8
	Port 4	4/Port N+8
Mezzanine 3 côté A	Port 1	3/Port N+12
	Port 2	4/Port N+12
	Port 3	3/Port N+4
	Port 4	4/Port N+4
Mezzanine 4 côté B	Port 1	3/Port N+7
	Port 2	4/Port N+7
	Port 3	3/Port N-1
	Port 4	4/Port N-1
Mezzanine 5 côté B	Port 1	2/Port N+3
	Port 2	2/Port N+11
	Port 3	2/Port N-1
	Port 4	2/Port N+7
Mezzanine 6 côté B	Port 1	1/Port N-1
NIC uniquement	Port 2	1/Port N+7
Mezzanine 7 côté B	Port 1	3/Port N+11
	Port 2	4/Port N+11
	Port 3	3/Port N+3
	Port 4	4/Port N+3

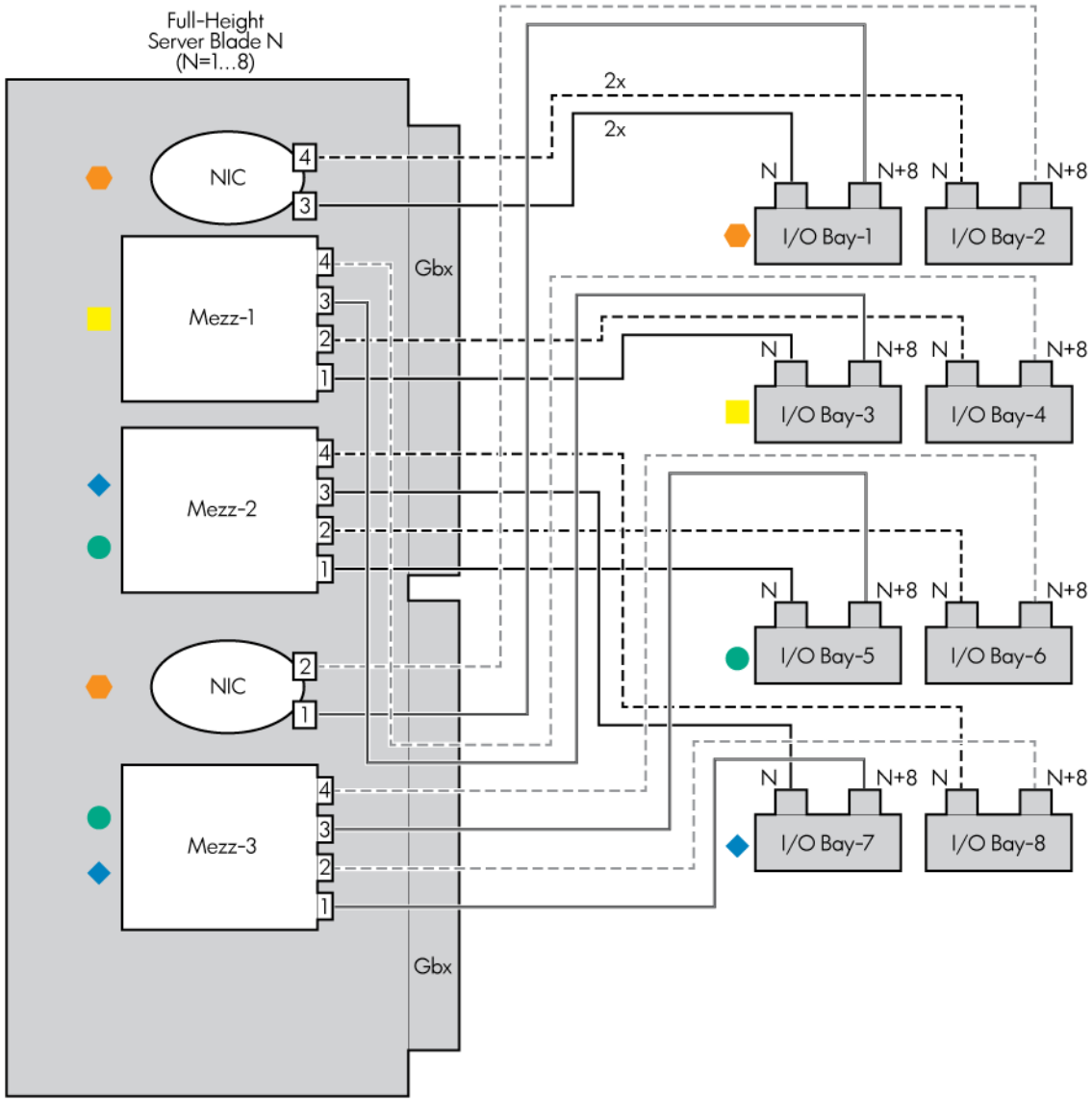
Vue graphique de mappage de ports de baie de périphérique pour boîtier c7000

Lames de serveur demi-hauteur, simple largeur (par exemple, des serveurs HP ProLiant BL260c, BL280c, BL420c, BL460c, BL465c, BL490c, BL495c et WS460c)



Dans ce diagramme, N correspond au numéro de la lame de serveur dans le boîtier et au numéro de port sur le commutateur. Par exemple, si une lame de serveur est insérée dans le connecteur 1, elle est considérée comme étant le périphérique 1 et les ports qui seront utilisés dans le commutateur 1 et le commutateur 2 sont les ports 1 et 1, respectivement. Pour une lame de serveur insérée dans le connecteur 2, les ports utilisés sur les commutateurs 1 et 2 seraient alors 2 et 2. Cette convention change pour les lames de serveur pleine hauteur dans le diagramme suivant.

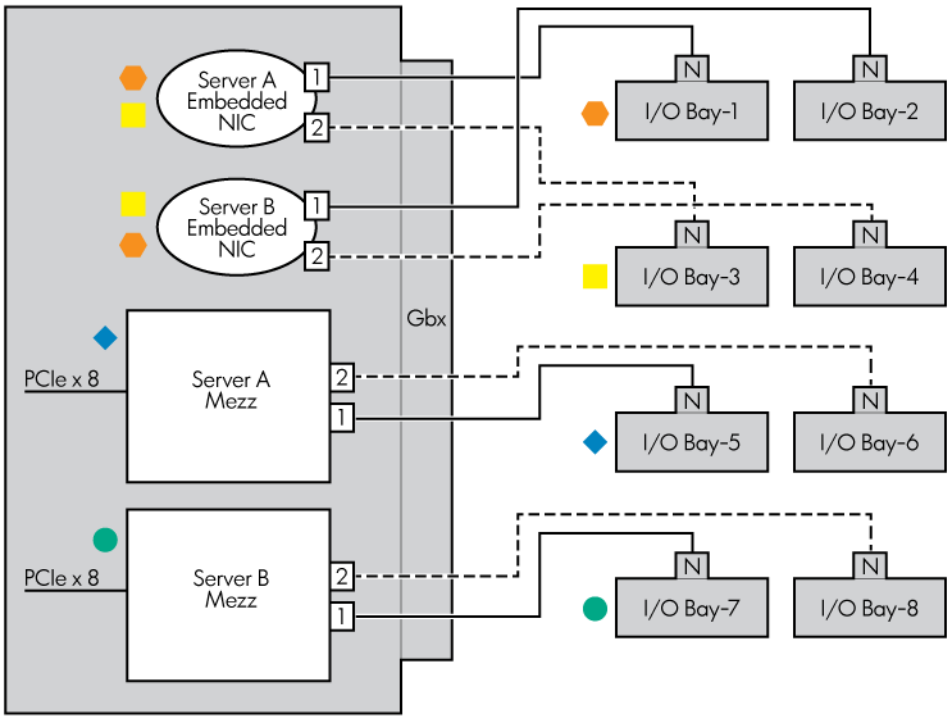
Lames de serveur pleine hauteur, simple largeur (telles que HP ProLiant BL680c (G1), BL680c Gen5 et BL480c BL620c, BL660c et BL685c)



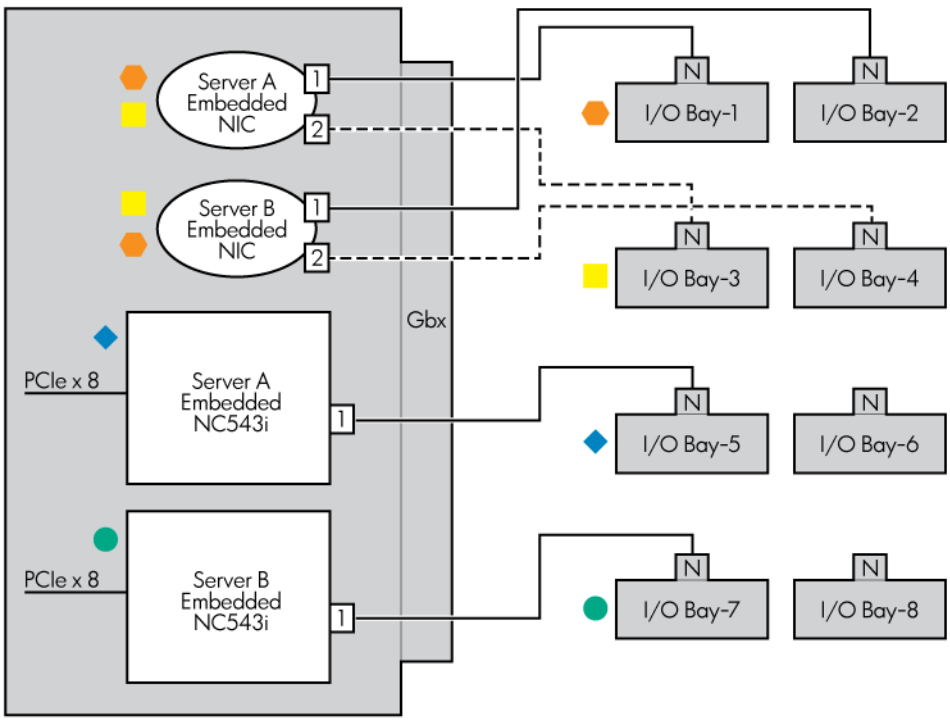
Dans ce diagramme, N correspond au numéro de la lame dans le boîtier et au numéro de port du commutateur. Par exemple, si une lame est insérée dans le connecteur 1, elle est considérée comme le périphérique 1. En raison de l'espace de deux lames de serveur demi-hauteur, simple largeur pris par les lames de serveur pleine hauteur, le boîtier est limité au maximum à huit lames de serveur pleine hauteur, simple largeur. Le mappage des ports de ces lames de serveur pleine hauteur, simple largeur peut apparaître comme différent de celui des lames de serveur demi-hauteur, mais tous deux utilisent des conventions très semblables.

Comme dans une lame de serveur demi-hauteur, si une lame est insérée dans le connecteur 1, elle est considérée comme le périphérique 1, mais elle possède un second ensemble de ports qui sera également mappé aux commutateurs 1 et 2. Avec la lame de serveur pleine hauteur, simple largeur, un schéma N/N+8 est utilisé sur les commutateurs. Par conséquent, la lame de serveur 1 sera mappée sur les ports 1 et 9 sur les deux commutateurs, puisque N=1. Pour une lame de serveur insérée dans le connecteur 2, les quatre ports utilisés sur les commutateurs 1 et 2 seraient alors 2 et 10, puisque N=2.

Lames de serveur demi-hauteur, double densité, telles que HP ProLiant BL2x220c (G1)–G6

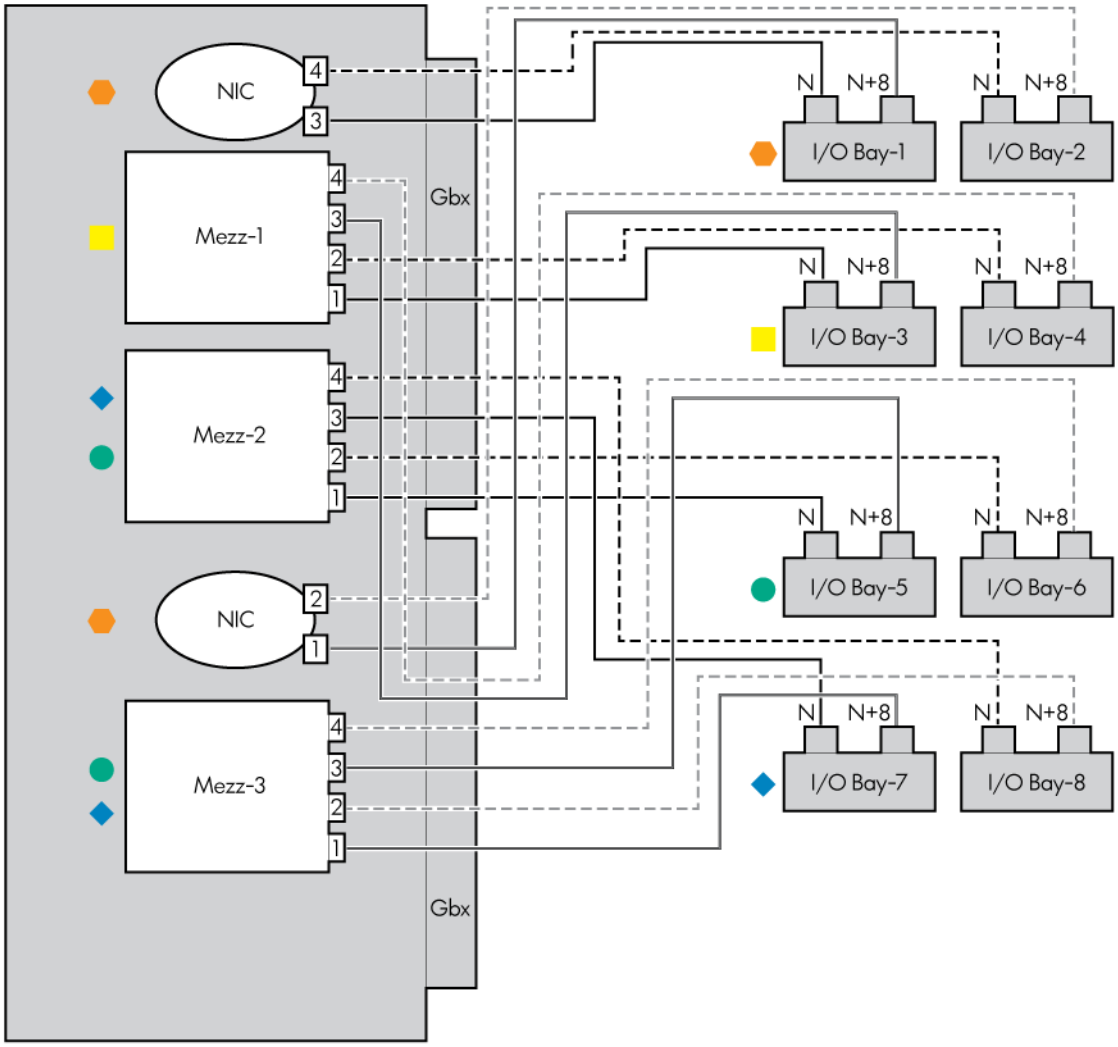


Lames de serveur demi-hauteur, double densité, telles que HP ProLiant BL2x220c G7



Lames de serveur pleine hauteur, double largeur telles que HP ProLiant BL680c G7

Côté A


NIC
4
3
Mezz-1
4
3
2
1
Gbx
Mezz-2
4
3
2
1
NIC
2
1
Mezz-3
4
3
2
1
Gbx
N
N+8
I/O Bay-1
I/O Bay-2
I/O Bay-3
I/O Bay-4
I/O Bay-5
I/O Bay-6
I/O Bay-7
I/O Bay-8

Côté B

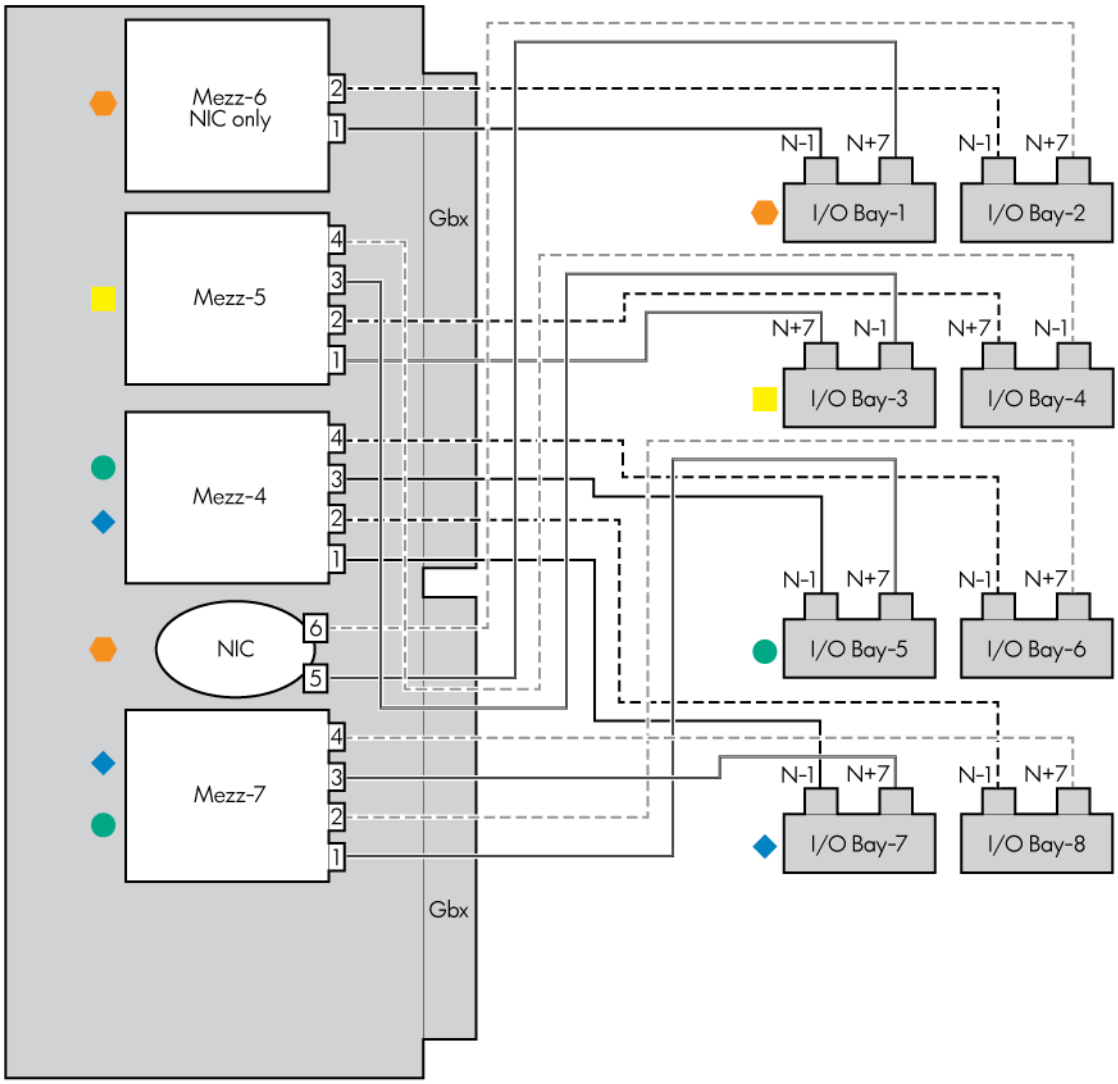


Tableau de mappage de ports de baie de périphérique pour boîtier c7000

Les lames de serveur sont reliées aux baies d'interconnexion de la manière suivante : Le terme 1x, 2x ou 4x désigne le nombre de voies d'interconnexion par port fournies par le contrôleur. Si aucun périphérique n'est présent, la case à cocher est désactivée et le port ne peut pas être affiché.

- Des exemples de ports 1x incluent 1GB Ethernet (1 GbE), 10GB Ethernet (10 GbE) et tous les périphériques Fibre Channel.
- Des exemples de ports 2x incluent 20GB Ethernet (20 GbE) et tous les périphériques SCSI (SAS) connectés en série.
- Des exemples de ports 4x incluent tous les périphériques InfiniBand.
- Les tableaux suivants font référence aux ports Ethernet en tant que cartes réseau.

Lames de serveur demi-hauteur, simple largeur

Le tableau suivant répertorie le mappage de ports pour des lames de serveur demi-hauteur installées dans une baie de périphérique demi-hauteur N (1-16) de boîtier c7000. Des exemples de lames de

serveur demi-hauteur comprennent les serveurs HP ProLiant BL260c, BL280c, BL420c, BL460c, BL465c, BL490c, BL495c et WS460c.

Connexion	Numéro de port	Connexion à baie d'interconnexion/port	Remarques
Carte réseau[1]	Carte réseau 1	1/Port N	Un ou deux modules d'interconnexion Ethernet simple largeur
	Carte réseau 2	2/Port N	
Connecteur mezzanine 1 — cartes 1x ou 2x	Port 1 1x/1x	3/Port N	• Un module d'interconnexion simple largeur • Quatre cartes de ports connectent uniquement les deux premiers ports.
	Port 2 1x/2x	4/Port N	
Connecteur mezzanine 1 — cartes 4x	Port 1 4x	3/Port N	• Un module d'interconnexion double largeur • Seul le port 1 d'une carte à deux ports sera connecté.
Connecteur mezzanine 2 — cartes 1x ou 2x	Port 1 1x/1x	5/Port N	Un ou deux modules d'interconnexion de largeur simple
	Port 2 1x/2x	6/Port N	
	Port 3 1x/2x	7/Port N[2]	
	Port 4 1x/2x	8/Port N[2]	
Connecteur mezzanine 2 — cartes 4x	Port 1 4x	5/Port N	Un ou deux modules d'interconnexion double largeur
	Port 2 4x	7/Port N[2]	

[1] Les lames de serveur G7 et de générations antérieure incluent des ports Ethernet intégrés sur la carte mère. Avec les lames de serveur Gen8 et de générations ultérieures, les ports Ethernet sont situés sur une carte sélectionnable par l'utilisateur appelée une carte (adaptateur) FlexibleLOM. Les ports de carte FlexibleLOM et les ports de carte réseau intégré ont le même mappage.
[2] La connectivité aux baies d'interconnexion 7 et 8 est uniquement disponible avec des cartes mezzanine à quatre ports ou le port 2 d'une carte 4x dans le connecteur mezzanine 2.

Lames de serveur demi-hauteur, double densité

Le tableau suivant répertorie les configurations disponibles pour des lames de serveur double densité installées dans une baie de périphérique demi-hauteur N (1-16) de boîtier c7000. Des exemples de ces lames de serveur double densité comprennent les serveurs HP ProLiant BL2x220c (G1) - G6.

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
Carte réseau intégrée de serveur A	Carte réseau intégrée 1 (Port: 1)	1/Port N
	Carte réseau intégrée 2 (Port: 2)	3/Port N
Carte mezzanine de serveur A	Port 1	5/Port N
	Port 2	6/Port N
Carte réseau intégrée de serveur B	Carte réseau intégrée 1 (Port: 1)	2/Port
	Carte réseau intégrée 2 (Port: 2)	4/Port N
Carte mezzanine de serveur B	Port 1	7/Port N

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
	Port 2	8/Port N

Lames de serveur demi-hauteur, double densité telles que HP ProLiant BL2x220c G7

Le tableau suivant répertorie les configurations disponibles pour des lames de serveur double densité, telles que ProLiant BL2x220c G7, installées dans une baie de périphérique demi-hauteur N (1-16) de boîtier c7000.

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
Carte réseau intégrée de serveur A	Carte réseau intégrée 1 (Port: 1)	1/Port N
	Carte réseau intégrée 2 (Port: 2)	3/Port N
Carte NC543i* intégrée de serveur A	Port 1	5/Port N
Carte réseau intégrée de serveur B	Carte réseau intégrée 1 (Port: 1)	2/Port N
	Carte réseau intégrée 2 (Port: 2)	4/Port N
Carte NC543i* intégrée de serveur B	Port 1	7/Port N

***** La carte NC543i intégrée de lame de serveur HP ProLiant BL2x220c G7 est automatiquement configurée par le module Onboard Administrator pour Ethernet, si un module d'interconnexion Ethernet est installé dans la baie 3, ou pour InfiniBand si une interconnexion InfiniBand double largeur est installée dans la baie 3. Pour changer la configuration NC543i d'un type à un autre, mettez hors tension toutes les lames de serveur HP ProLiant BL2x220c G7 et remplacez le module d'interconnexion par l'autre type. Redémarrez le module Onboard Administrator actif ou réinstallez toutes les lames de serveur HP ProLiant BL2x220c G7 : le module Onboard Administrator reconfigure toutes les cartes NC543i intégrées pour le nouveau type d'interconnexion.

Lame d'extension E/S AMC Telco

Le tableau suivant répertorie les configurations disponibles pour des périphériques AMC Telco installés dans une baie de périphérique N (1-16) de boîtier c7000.

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
Lame AMC intégrée (1)	Port 1	1/Port N
	Port 2	2/Port N
	Port 3	3/Port N
	Port 4	4/Port N
Lame AMC intégrée (2)	Port 5	5/Port N
	Port 6	6/Port N
	Port 7	7/Port N
	Port 8	8/Port N

Lames de serveur pleine hauteur, double largeur telles que le serveur HP ProLiant BL680c G7

Le tableau suivant répertorie le mappage de ports pour des lames de serveur pleine hauteur, double largeur telles que HP ProLiant BL680c G7 installées dans une baie de périphérique pleine hauteur c7000 N (2, 4, 6 ou 8).

Connexion	Numéro de port	Connexion à baie d'interconnexion/port
Carte réseau intégrée côté A	Carte réseau 1	1/Port N+8
	Carte réseau 2	2/Port N+8
	Carte réseau 3	1/Port N
	Carte réseau 4	2/Port N
Carte réseau intégrée côté B	Carte réseau 5	1/Port N+7
	Carte réseau 6	2/Port N+7
Mezzanine 1 côté A	Port 1	3/Port N
	Port 2	4/Port N
	Port 3	3/Port N+8
	Port 4	4/Port N+8
Mezzanine 2 côté A	Port 1	5/Port N
	Port 2	6/Port N
	Port 3	7/Port N
	Port 4	8/Port N
Mezzanine 3 côté A	Port 1	7/Port N+8
	Port 2	8/Port N+8
	Port 3	5/Port N+8
	Port 4	6/Port N+8
Mezzanine 4 côté B	Port 1	7/Port N-1
	Port 2	8/Port N-1
	Port 3	5/Port N-1
	Port 4	6/Port N-1
Mezzanine 5 côté B	Port 1	3/Port N+7
	Port 2	4/Port N+7
	Port 3	3/Port N-1
	Port 4	4/Port N-1
Mezzanine 6 côté B	Port 1	1/Port N-1
NIC uniquement	Port 2	2/Port N-1
Mezzanine 7 côté B	Port 1	5/Port N+7
	Port 2	6/Port N+7
	Port 3	7/Port N+7
	Port 4	8/Port N+7

Microprogrammes

Pour afficher les informations de microprogramme pour les composants de la baie de périphérique et effectuer une opération de détection manuelle et mise à jour manuelle de microprogramme, cliquez

sur **Firmware**. Pour plus d'informations sur les problèmes de performances et les exigences de prise en charge, consultez la section « Enclosure Firmware Management » (Enclosure Firmware Management à la page 195).

Informations récapitulatives des microprogrammes

Rangée	Description
Bay (Baie)	Baie du périphérique dans le boîtier.
Device Model (Modèle du périphérique)	Numéro de modèle du périphérique.
Firmware Component (Composant du microprogramme)	Composant pour lequel les informations relatives aux microprogrammes sont fournies.
Current Version (Version actuelle)	Version du microprogramme installé sur le composant.
Firmware ISO Version (Version ISO du microprogramme)	Dernière version du microprogramme disponible pour installation sur le composant.

REMARQUE : si le microprogramme de la lame ne correspond pas au microprogramme de l'image ISO du DVD une fois un serveur détecté ou mis à jour, une icône d'information s'affiche.

REMARQUE : Une lettre incluse après la version du microprogramme indique une révision de note de version du composant intelligent. Cette révision n'est pas une mise à jour fonctionnelle du microprogramme.

Détection manuelle

Une détection manuelle effectue un démarrage pour réaliser une détection sur le serveur, recueille des informations étendues relatives aux microprogrammes de ce serveur et redémarre le serveur en fonctionnement normal.

Pour lancer le processus de détection sur le serveur sélectionné, cliquez sur **Start Manual Discovery** (Lancer la détection manuelle).

Si Secure Boot est configuré sur la lame de serveur, vous ne pouvez pas effectuer une détection manuelle. Le bouton **Start Manual Discovery** apparaît en grisé. Le mode Secure Boot empêche les utilisateurs (y compris l'administrateur) d'effectuer cette opération à partir de la carte iLO ou du système d'exploitation ou de la lame de serveur. Les opérations d'amorçage peuvent être effectuées uniquement à partir du périphérique d'amorçage configuré dans le BIOS par l'administrateur.

Mise à jour manuelle

Une mise à jour manuelle effectue un démarrage pour réaliser une mise à jour sur le serveur, met à jour le microprogramme de ce serveur, puis redémarre le serveur en fonctionnement normal.

Pour lancer le processus de mise à jour sur le serveur sélectionné, cliquez sur **Start Manual Update** (Lancer la mise à jour manuelle).

Si Secure Boot est configuré sur la lame de serveur, vous ne pouvez pas effectuer une mise à jour manuelle. Le bouton **Lancer la mise à jour manuelle** apparaît en grisé. Le mode Secure Boot empêche les utilisateurs (y compris l'administrateur) d'effectuer cette opération à partir de la carte iLO ou du système d'exploitation ou de la lame de serveur. Les opérations d'amorçage peuvent être effectuées uniquement à partir du périphérique d'amorçage configuré dans le BIOS par l'administrateur.

Pour plus d'informations sur la détection manuelle et la mise à jour manuelle, consultez la section « Initiation d'une mise à jour ou détection manuelle » (Initiation d'une mise à jour ou détection manuelle à la page 276).

Journal des microprogrammes

Ce journal affiche des informations détaillées sur la dernière opération Enclosure Firmware Management effectuée sur le serveur. Ce journal est spécifique au serveur et il est effacé chaque fois qu'une nouvelle opération Enclosure Firmware Management est initiée sur le serveur. Ce journal est également effacé lorsque le serveur est retiré du boîtier et lorsqu'il est défini en mode usine.

Le journal du microprogramme est la ressource la plus utile pour déterminer l'état d'avancement d'une opération Enclosure Firmware Management sur un serveur particulier.

Pour plus d'informations sur le journal du microprogramme, consultez la section « Consignation » (Journaux de gestion des microprogrammes à la page 280).

Journal de session

Ce journal affiche des informations détaillées sur la dernière opération Enclosure Firmware Management effectuée sur le serveur et consigne toute la session dans le VSP iLO. Ce journal est spécifique au serveur et est effacé chaque fois qu'une nouvelle opération Enclosure Firmware Management est initiée sur le serveur. Ce journal est également effacé lorsque le serveur est retiré du boîtier.

Pour plus d'informations sur le journal de session, consultez la section « Consignation » (Journaux de gestion des microprogrammes à la page 280).

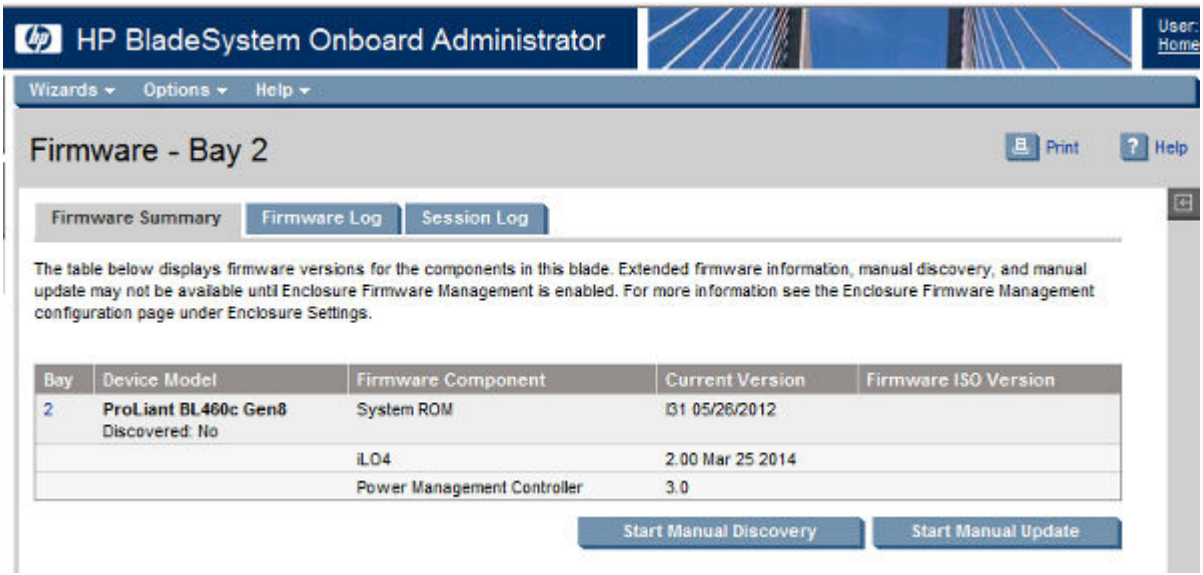
Initiation d'une mise à jour ou détection manuelle

ATTENTION : Il est possible que la mise à jour de Enclosure Firmware Management à l'aide d'une image SPP de taille supérieure à 4 Go et hébergée à partir d'un serveur Web ne fonctionne pas correctement.

REMARQUE : Lorsqu'une tâche Enclosure Firmware Management est en cours, ne redémarrez pas le module Onboard Administrator. Évitez de mettre la lame hors tension ou de la retirer du boîtier.

REMARQUE : Si Secure Boot est configuré sur la lame de serveur, vous ne pouvez pas effectuer une opération de détection manuelle ou de mise à jour manuelle. Les boutons **Start Manual Discovery** et **Start Manual Update** sont grisés. Le mode Secure Boot empêche les utilisateurs (y compris l'administrateur) d'effectuer ces opérations à partir de la carte iLO ou du système d'exploitation de la lame de serveur. Les opérations d'amorçage peuvent être effectuées uniquement à partir du périphérique d'amorçage configuré dans le BIOS par l'administrateur.

Serveurs individuels



Pour initier une opération de mise à jour ou détection manuelle sur des serveurs individuels :

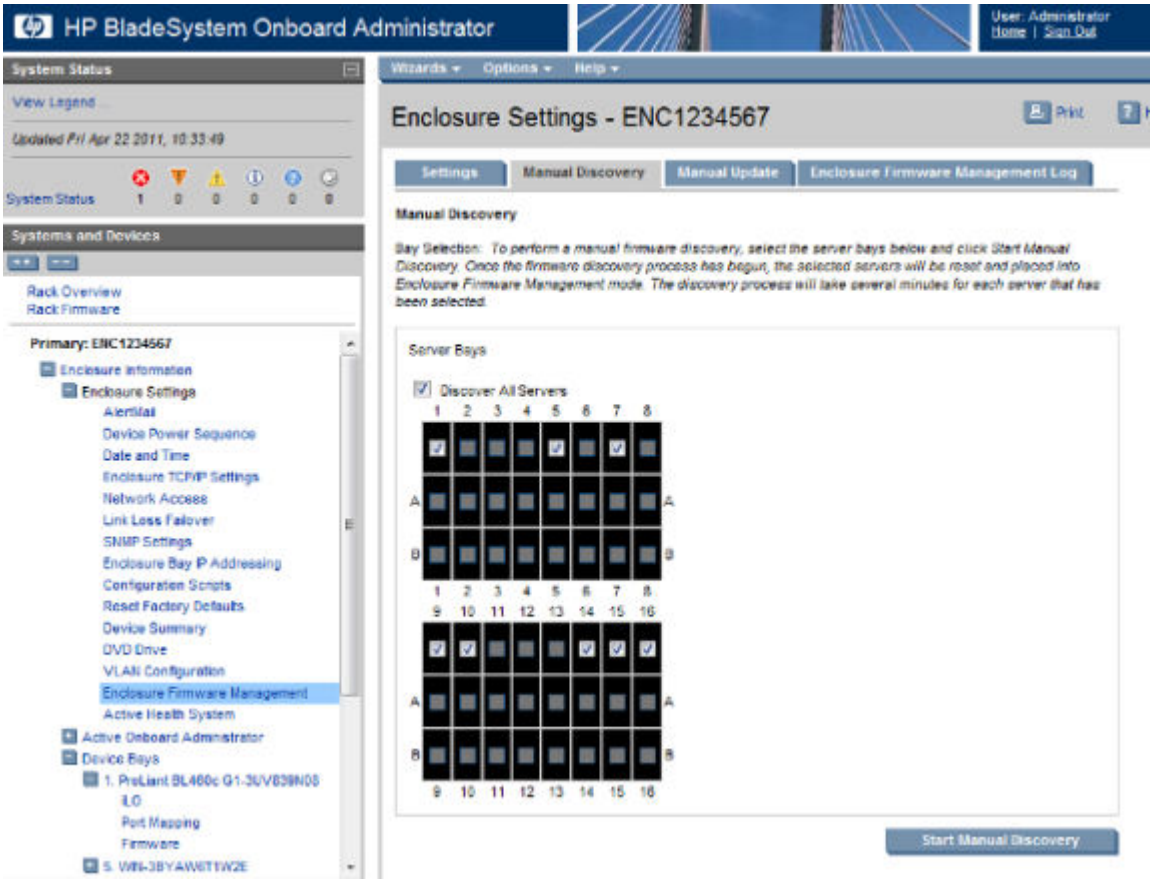
1. Sélectionnez **Device Bays** (Baies de périphériques) dans l'arborescence de gauche. Sélectionnez la baie à afficher, puis sélectionnez **Firmware** (Microprogrammes).
2. Cliquez sur **Start Manual Discovery** (Lancer la découverte manuelle) ou sur **Start Manual Update** (Lancer la mise à jour manuelle).

Plusieurs serveurs

Pour initier une opération de détection manuelle sur plusieurs serveurs :

1. Dans l'arborescence de gauche, sélectionnez **Enclosure Settings>Enclosure Firmware Management**.

2. Sélectionnez l'onglet **Manual Discovery** (Détection manuelle).

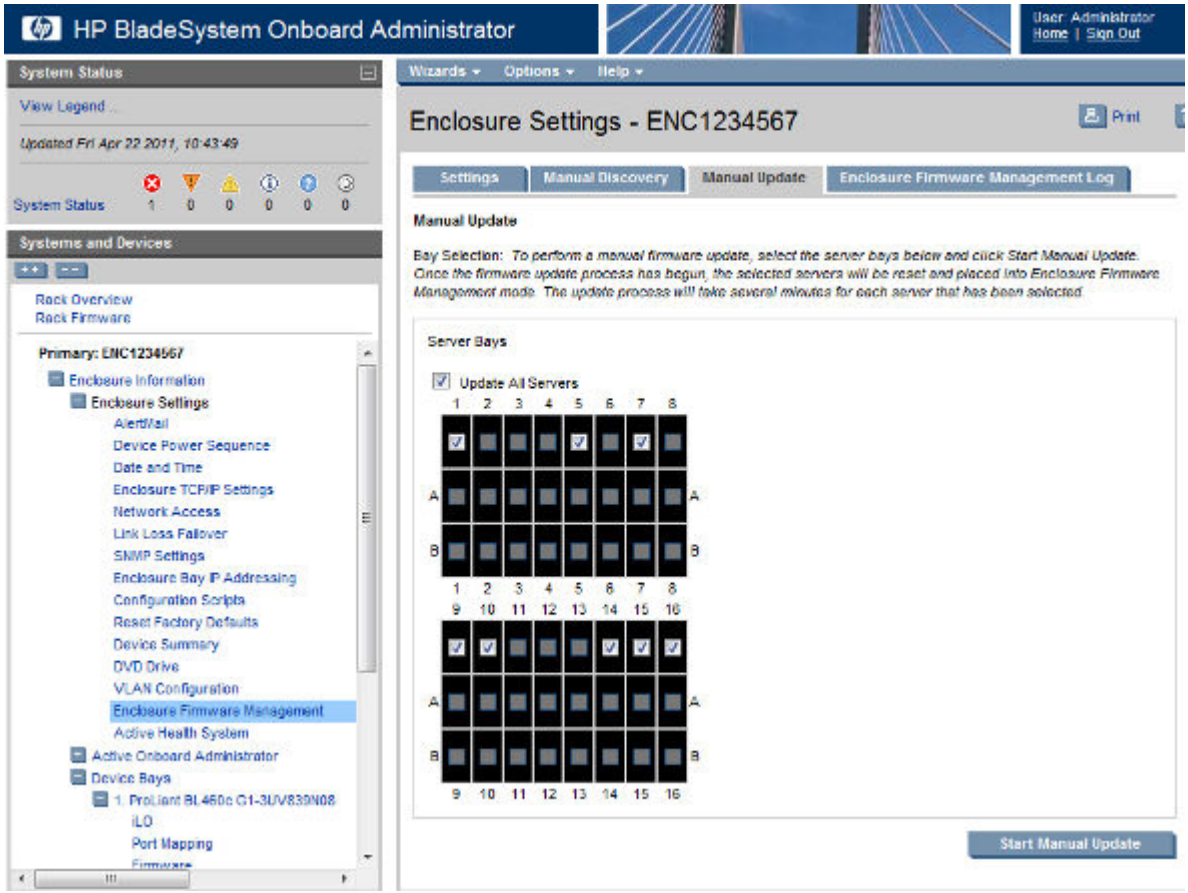


3. Cochez la case en regard des baies de serveur appropriées ou sélectionnez la case **Discover All Servers** (Détecter tous les serveurs).
4. Cliquez sur **Start Manual Discovery** (Lancer la découverte manuelle).

Pour initier une mise à jour manuelle sur plusieurs serveurs :

1. Dans l'arborescence de gauche, sélectionnez **Enclosure Settings>Enclosure Firmware Management**.

2. Sélectionnez l'onglet **Manual Update** (Mise à jour manuelle).

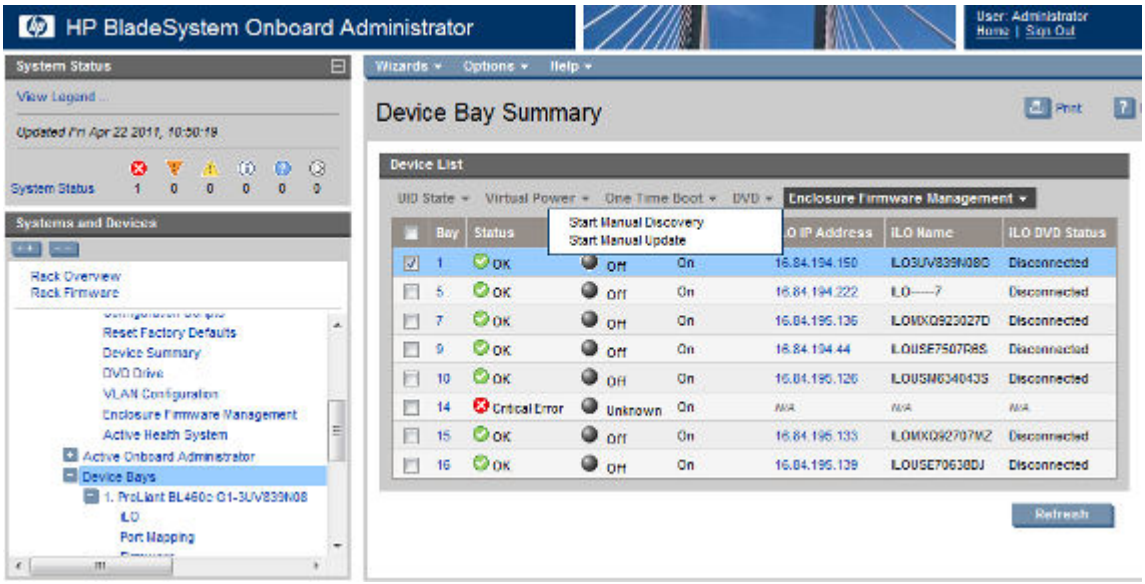


3. Cochez la case en regard des baies de serveurs appropriées ou sélectionnez la case **Update All Servers** (Mettre à jour tous les serveurs).
4. Cliquez sur **Start Manual Update** (Lancer la mise à jour manuelle).

Pour initier une opération de détection ou de mise à jour manuelle à partir de l'écran Device Bays (Baies de périphériques) :

1. Dans l'arborescence de gauche, sélectionnez **Device Bays** (Baies de périphériques).
2. Cochez la case en regard de la baie appropriée.

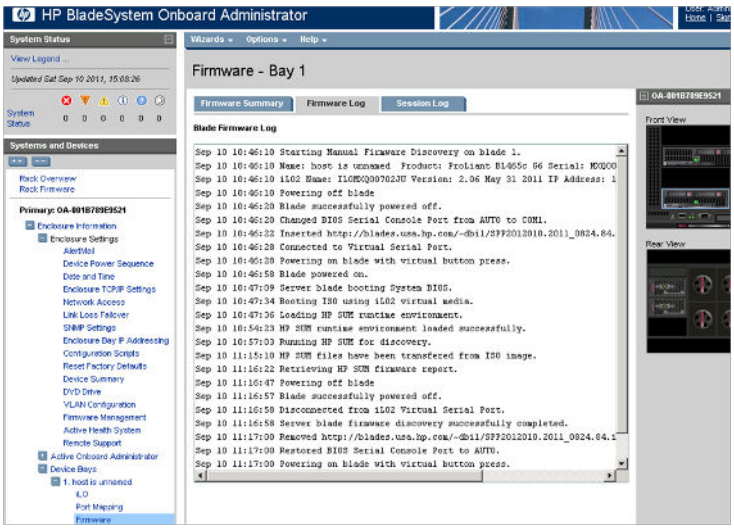
3. Dans le menu Firmware Management (Gestion des microprogrammes), sélectionnez **Start Manual Discovery** (Lancer la découverte manuelle) ou **Start Manual Update** (Lancer la mise à jour manuelle).



Journaux de gestion des microprogrammes

Les événements de l'utilitaire Enclosure Firmware Management sont écrits dans trois journaux. Les sections suivantes décrivent le type d'événements intégrés dans chaque journal. Tous les journaux peuvent être utilisés pour vérifier l'état d'avancement d'une tâche ou à des fins de dépannage.

Journal des microprogrammes

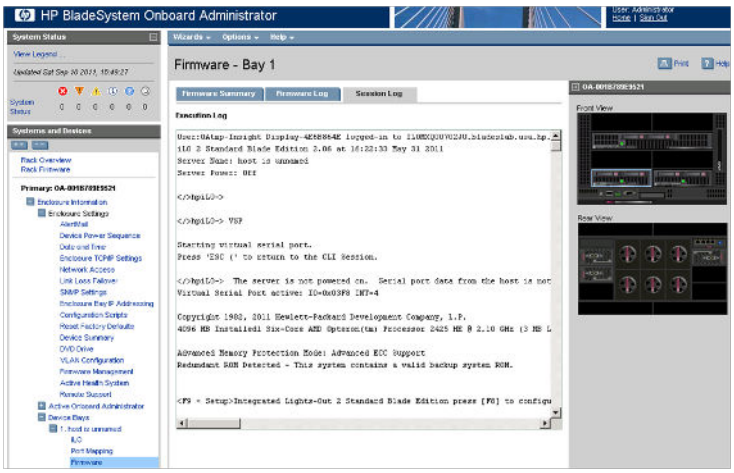


Ce journal affiche des informations détaillées sur la dernière opération Enclosure Firmware Management effectuée sur le serveur. Ce journal est spécifique au serveur et il est effacé chaque fois qu'une nouvelle opération Enclosure Firmware Management est initiée sur le serveur. Ce journal est également effacé lorsque le serveur est retiré du boîtier et lorsqu'il est défini en mode usine.

Ce journal est conservé entre les réamorçages OA et les pertes d'alimentation. Il est conservé sur le module OA en mode Standby, s'il est présent.

Le journal du microprogramme est la ressource la plus utile pour déterminer l'état d'avancement d'une opération Enclosure Firmware Management sur un serveur particulier.

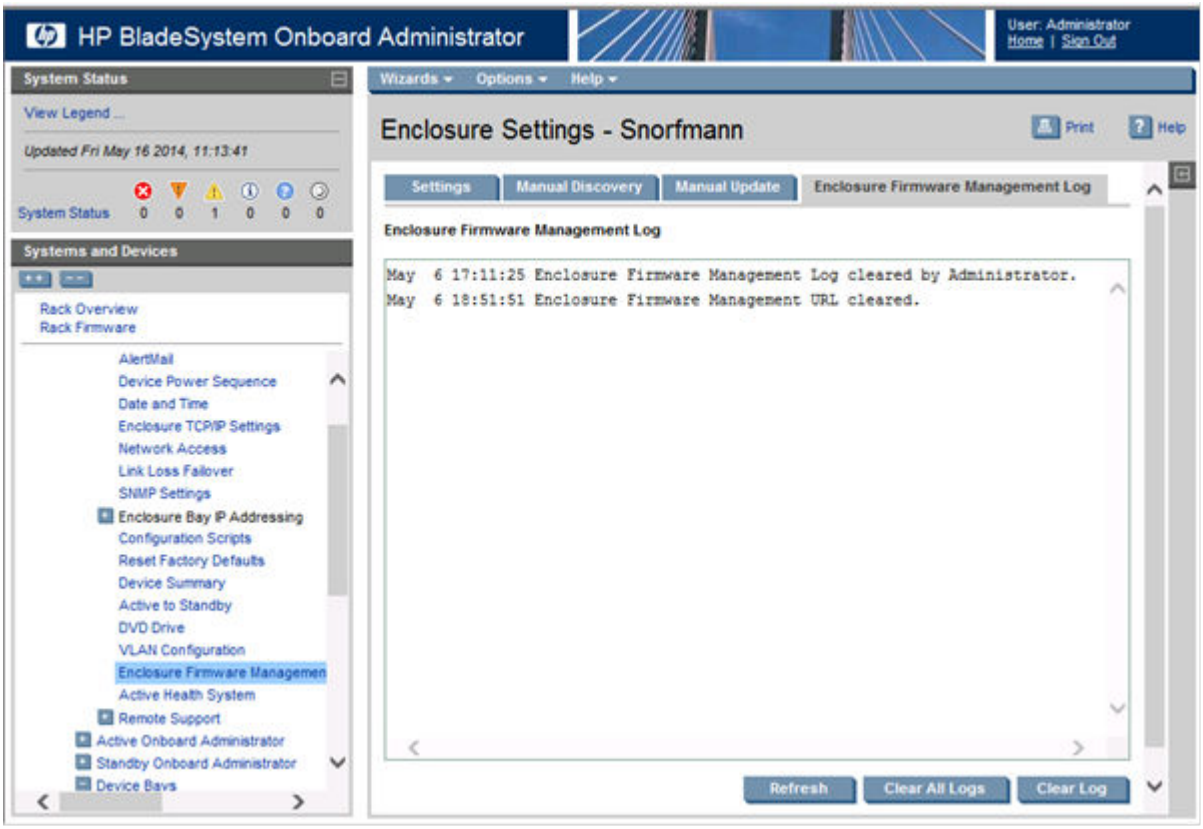
Journal de session



Ce journal affiche des informations détaillées sur la dernière opération Enclosure Firmware Management effectuée sur le serveur et consigne toute la session dans le VSP iLO. Ce journal est spécifique au serveur et est effacé chaque fois qu'une nouvelle opération Enclosure Firmware Management est initiée sur le serveur. Ce journal est également effacé lorsque le serveur est retiré du boîtier.

Ce journal est conservé entre les réamorçages OA et les pertes d'alimentation. Il est conservé sur le module OA en mode Standby, s'il est présent.

Journal Enclosure Firmware Management



Le journal Enclosure Firmware Management offre une vue d'ensemble des principaux événements de l'utilitaire Enclosure Firmware Management, tels que les sélections d'images de microprogramme, les modifications programmées ou liées aux politiques et les opérations de microprogramme initiées et terminées. Ce journal ne contient pas les détails inclus dans le journal des microprogrammes pour chaque serveur.

Le journal Enclosure Firmware Management est conservé entre les réamorçages OA et les pertes d'alimentation. Il est conservé sur le module OA en mode Standby, s'il est présent.

Pour visualiser des informations de journal mises à jour, cliquez sur **Refresh** (Actualiser).

Pour effacer les informations concernant le journal Enclosure Firmware Management et le journal des microprogrammes spécifiques au serveur et le journal de session, cliquez sur **Clear All Logs** (Effacer tous les journaux).

Pour effacer les informations concernant le journal Enclosure Firmware Management, cliquez sur **Clear Log** (Effacer le journal).

⚠ **ATTENTION :** Une fois supprimées, ces données ne peuvent pas être restaurées.

Pour plus d'informations sur les échecs d'événements, consultez la section « Journal Enclosure Firmware Management » (Journal Enclosure Firmware Management à la page 203).

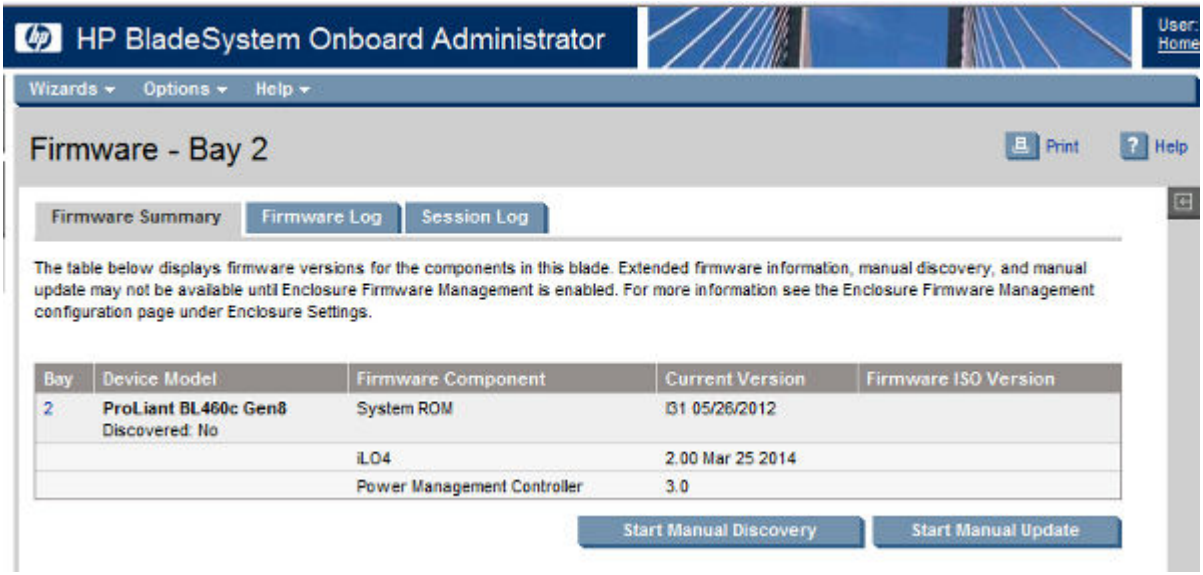
Affichage des versions des microprogrammes

Une fois la tâche Enclosure Firmware Management terminée, vérifiez la version des microprogrammes de tous les périphériques sélectionnés pour une mise à jour. Une tâche Enclosure Firmware Management menée à terme n'indique pas que des microprogrammes ont été mis à jour aux versions de l'image ISO. Pour plus d'informations, consultez la section « Microprogramme » (Variations de versions de microprogrammes à la page 284).

Microprogramme de serveur

Sélectionnez **Device Bays** (Baies de périphériques) dans l'arborescence de gauche. Sélectionnez la baie à afficher, puis cliquez sur **Firmware** (Microprogrammes).

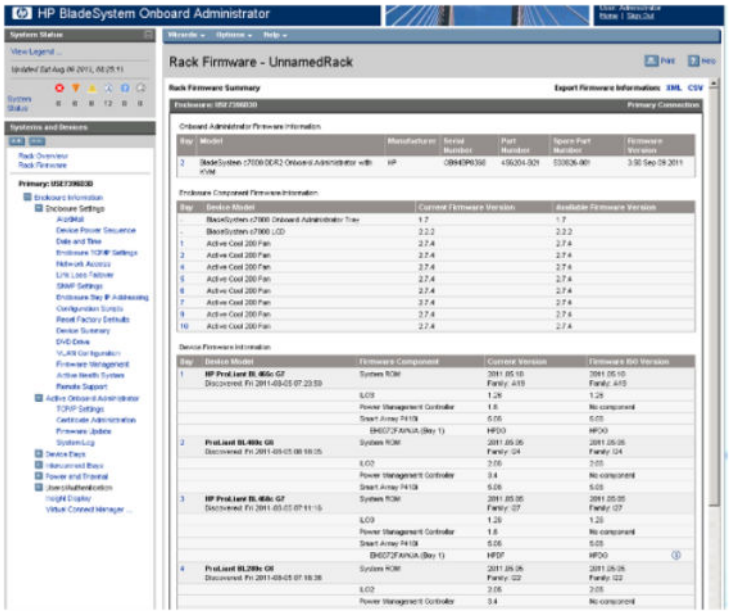
Les informations détaillées relatives aux microprogrammes du serveur s'affichent dans l'interface utilisateur graphique et la ligne de commande pour chaque serveur. Il existe pour chaque lame de serveur un journal de gestion des microprogrammes où sont consignées toutes les étapes de la dernière mise à jour ou opération de détection des microprogrammes, et les informations récapitulatives des microprogrammes affichent la date et l'heure de la dernière mise à jour ou opération de détection. Si la lame de serveur est retirée du boîtier, ce journal est effacé. Ces journaux sont synchronisés au module Onboard Administrator en Standby, s'il y en a un et les journaux sont stockés dans une mémoire flash afin que les informations demeurent disponibles après un redémarrage du module Onboard Administrator.



Rack firmware (Microprogrammes du rack)

Sélectionnez **Rack Firmware** (Microprogrammes du rack) en haut du volet de l'arborescence de gauche.

L'interface utilisateur graphique ou la ligne de commande du module Onboard Administrator fournit un rapport contenant l'inventaire des microprogrammes actuellement présents dans chaque boîtier. Pour les boîtiers liés, l'interface utilisateur graphique fournit les microprogrammes présents au sein de tous les boîtiers liés. Le rapport comporte la version actuelle des microprogrammes du BIOS, iLO, PMC, de la carte réseau, FC HBA, Smart Array du serveur, ainsi que tous les disques durs installés et reliés à Smart Array. Ces informations sont une aide lors du diagnostic de problèmes réseau ou FC SAN complexes causés par des versions de microprogrammes NIC ou FC HBA incorrectes.



Variations de versions de microprogrammes

Les scénarios suivants sont susceptibles de laisser apparaître des versions de microprogrammes ou états irréguliers.

- Une lettre incluse après la version du microprogramme indique une révision de note de version du composant intelligent. Il ne s'agit pas d'une mise à jour fonctionnelle du microprogramme.
- Si `No Component` (Absence de composant) s'affiche comme version ISO du microprogramme, cela signifie que l'image SPP ne contient pas de microprogramme pour ce composant. Ce scénario se produit habituellement avec le contrôle de supervision d'alimentation sur les serveurs ProLiant G7.
- Si une icône d'information s'affiche, le microprogramme de la lame du serveur ne correspond pas au microprogramme de l'image ISO du DVD, après la détection ou la mise à jour d'un serveur.
- Si la carte réseau, FC HBA, Smart Array, ou les disques durs installés connectés à Smart Array sont programmés sans utiliser l'utilitaire Enclosure Firmware Management, le module Onboard Administrator ne peut pas interpréter ces informations et continue de donner les informations des microprogrammes sur la base des dernières opérations Enclosure Firmware Management.
- Si le microprogramme n'est pas mis à jour à l'aide de l'utilitaire Enclosure Firmware Management, suivi de l'utilitaire et de génération de rapports ne refléteront pas les modifications apportées à l'aide d'autres outils.

  Le suivi et les rapports EFM ne reflètent pas les modifications apportées à l'aide d'autres outils tels que HP SUM et HP SIM si le microprogramme sur une lame n'a été pas mis à jour à l'aide de l'utilitaire EFM. Les versions correctes du microprogramme seront rapportées une fois les opérations de détection ou de mise à jour de l'utilitaire EFM effectuées.

Lames de stockage

Dans le menu **Systems and Devices**, la catégorie Device Bays (Baies de périphérique) répertorie toutes les lames de serveur et lames de stockage. La sélection d'une option de menu de lame de stockage affiche la page d'état de cette dernière (la sélection du symbole **+** situé sur la gauche de l'option de menu ne développe pas la lame de stockage). Trois onglets sont disponibles pour afficher

des informations spécifiques à la lame de stockage : **Status** (État), **Information** (Informations) et **Virtual Devices** (Périphériques virtuels).

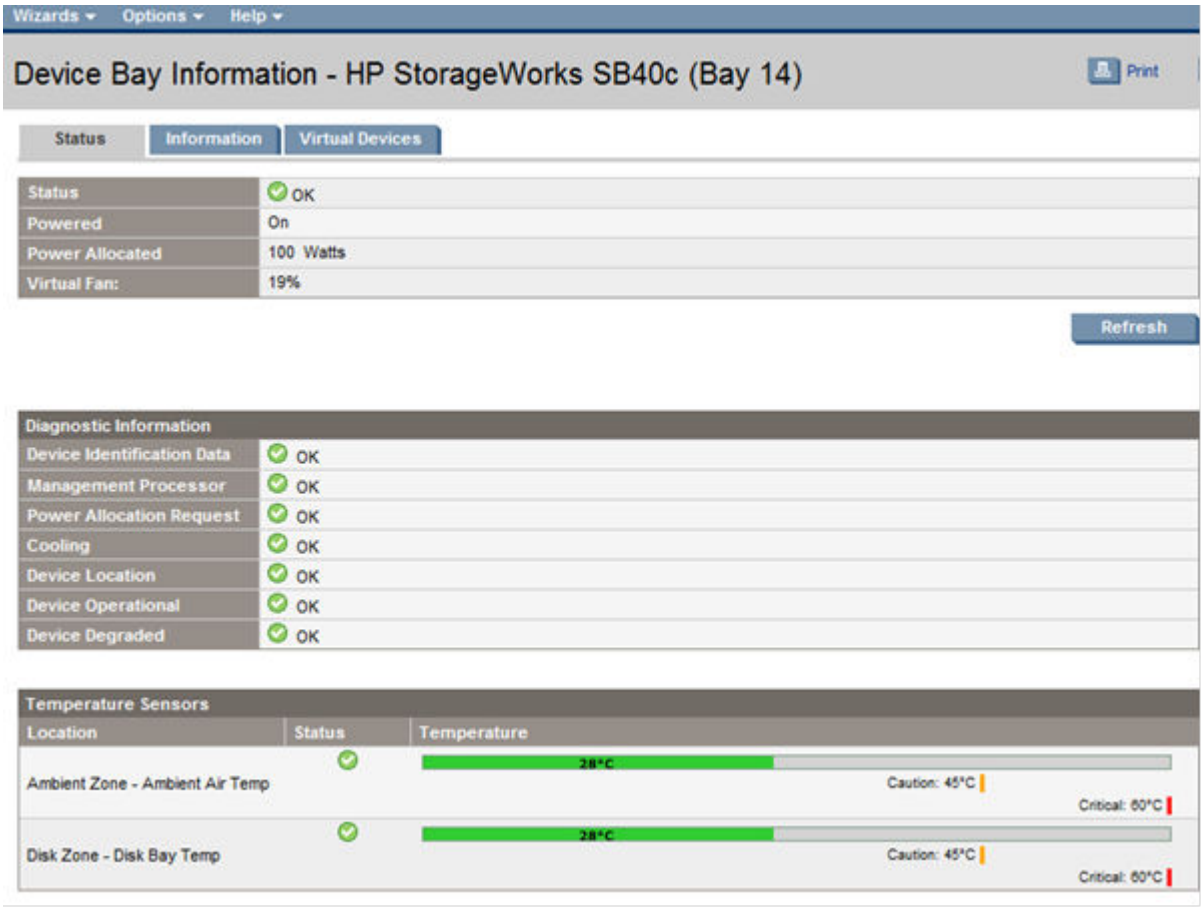
Les lames de stockage sont insérées dans le boîtier adjacent aux lames de serveur en suivant les règles de positionnement physique et en s'assurant que la lame de stockage est alimentée avant la mise sous tension et son association à une lame de serveur.

Lors de l'utilisation de lames de serveur demi-hauteur, la lame de stockage doit être placée dans le logement du boîtier situé sur la gauche de la lame de serveur. Pour chaque lame de serveur installée dans le boîtier, une lame de stockage associée peut être placée dans le boîtier sur la gauche de la lame de serveur (avec un maximum de huit lames de serveur et huit lames de stockage).

Lors de l'utilisation de lames de serveur pleine hauteur, la lame de stockage doit être placée dans le logement inférieur du boîtier sur la gauche de la lame de serveur. Le positionnement de la lame de stockage dans le logement supérieur gauche du boîtier entraîne une erreur de périphérique partenaire. Vous pouvez placer une lame de serveur demi-hauteur dans le logement supérieur gauche d'une lame de serveur pleine hauteur lorsqu'une lame de stockage est située sur la position inférieure gauche de la lame de serveur pleine hauteur.

Les lames de serveur pleine hauteur requièrent une carte mezzanine pour communiquer avec la lame de stockage appropriée. Si une lame de stockage est correctement placée à côté d'une lame de serveur pleine hauteur mais que cette dernière ne dispose pas de la carte mezzanine appropriée, une erreur de configuration, et non une erreur de périphérique partenaire, se produit.

En cas de déconnexion de l'alimentation d'une lame de serveur, l'alimentation de la lame de stockage associée est également déconnectée.



Rangée	Description
Status (État)	État global de la lame de stockage. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Failed (Échec).
Powered (Alimentée)	État d'alimentation de la lame de stockage. Les valeurs possibles sont On (Activé) et Off (Désactivé).
Power Allocated (Puissance allouée)	Puissance d'alimentation autorisée pour la lame de stockage, en watts.
Virtual Fan (Ventilateur virtuel)	Pourcentage de la vitesse maximum (RPM) du ventilateur virtuel.
Partner Device (Périphérique partenaire)*	Affiche la lame de serveur et la baie auxquelles la lame de stockage est associée.

* Non illustré

Informations de diagnostics

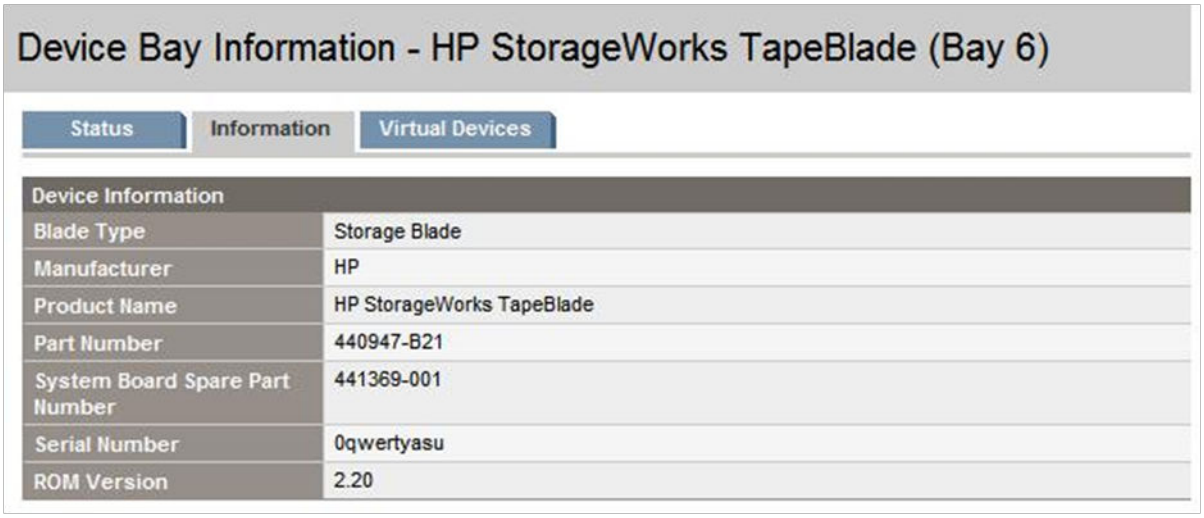
Les informations de diagnostics sont recueillies de deux façons : Par interrogation du microcontrôleur de périphérique (résultat d'un état détérioré si une panne s'est produite) ou envoyées par le microcontrôleur du périphérique, sans interrogation, pour signaler une panne.

Rangée	Description
Device Identification Data (Données d'identification du périphérique)	Contient des informations telles que le nom du modèle, la référence, le numéro de série, ainsi que d'autres informations utilisées pour identifier le périphérique. Ces données sont également appelées données FRU. Une erreur de données d'identification du périphérique s'affiche si les données sont absentes ou illisibles par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Management Processor (Processeur de gestion)	État du processeur d'interface de gestion du contrôleur de stockage. Les valeurs possibles sont OK et Error.
Temperature (Température)	La température est au-dessus du seuil d'avertissement. Les valeurs possibles sont OK et Temperature Warning (Avertissement de température).
Overheat Check (Contrôle de surchauffe)	La température est au-dessus du seuil de danger. Les valeurs possibles sont OK et Critical temperature threshold reached (Seuil critique de température atteint).
Power Allocation Request (Demande d'allocation d'alimentation)	La puissance est insuffisante pour alimenter cette lame de stockage correctement. Les valeurs possibles sont OK et Insufficient enclosure power (Alimentation de boîtier insuffisante).
Cooling (Refroidissement)	Le nombre de ventilateurs est insuffisant pour ventiler correctement cette lame de stockage ou la configuration des ventilateurs est incorrecte. Les valeurs possibles sont OK et Insufficient fans for enclosure cooling (Nombre de ventilateurs insuffisant pour refroidissement du boîtier).
Device Location (Emplacement du périphérique)	État de configuration de la baie de la lame de stockage. Les valeurs possibles sont OK et Incorrect location for proper device cooling (Emplacement incorrect pour refroidissement correct du périphérique).

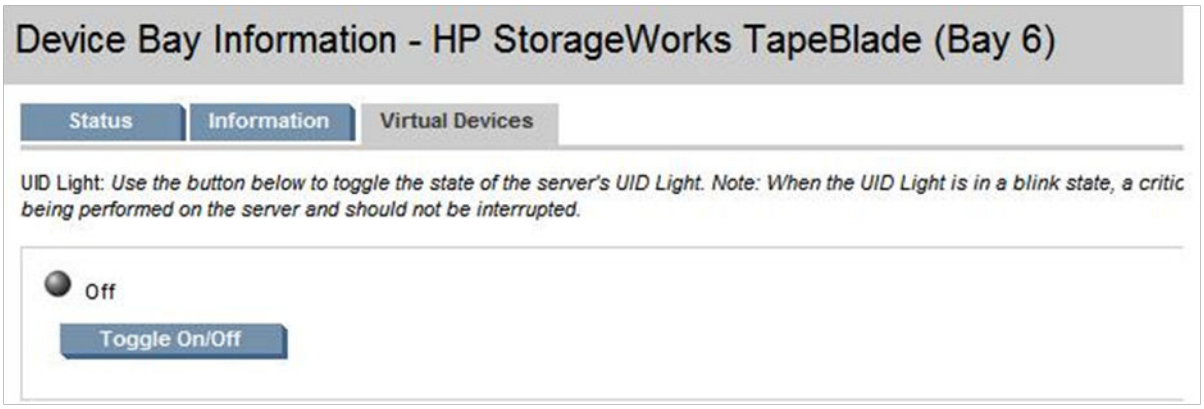
Rangée	Description
Device Operational (Périphérique fonctionnel)	État de la lame de stockage. Les valeurs possibles sont OK et Error.
Device Degraded (Périphérique détérioré)	Échec du périphérique. L'état a été demandé par le Onboard Administrator. Les valeurs possibles sont OK et Error.
Disk Tray (Tiroir de disques)	DVD Drive (Lecteur de CD/DVD-ROM). Les valeurs possibles sont Disk Tray is OPEN (Le tiroir de disques est OUVERT) ou Disk Tray is CLOSED (Le tiroir de disques est FERMÉ).
Partner Device Presence (Présence de périphérique partenaire)	La lame de stockage dispose d'un serveur associé. Il doit s'agir d'un serveur placé à côté de celle-ci dans la configuration correcte. Les valeurs possibles sont OK et No adjacent partner found (Aucun partenaire adjacent trouvé).
Power Sequence (Séquence d'alimentation)	La lame de stockage doit toujours être alimentée en premier. Si une lame de stockage est insérée à côté d'une lame de serveur déjà alimentée, l'alimentation est refusée. La lame de serveur doit être mise hors tension afin que la lame de stockage puisse être alimentée. La lame de serveur peut ensuite être mise sous tension. Les valeurs possibles sont OK et Potential partner device is already ON (Partenaire potentiel déjà alimenté).
Partner Device Link (Lien du périphérique partenaire)	En cas de dégradation, deux lames de stockage ont été placées côte à côte dans le boîtier. Les valeurs possibles sont OK et Inappropriate device in adjacent bay (Périphérique inapproprié dans baie adjacente).
Virtual Connect Configured (Connexion virtuelle configurée)	Les valeurs possibles sont Configured for Virtual Connect (Configurée pour connexion virtuelle) et Not configured for Virtual Connect (Non configurée pour connexion virtuelle).

Informations de capteurs de température

Colonne	Description
Emplacement	Emplacement du capteur dans le périphérique.
Status (État)	État du capteur de température. L'état correspond à la présentation graphique de la température
Temperature (Température)	Présentation graphique de la température.



Rangée	Description
Blade Type (Type de lame)	Type de périphérique installé dans la baie
Manufacturer (Fabricant)	Fabricant du périphérique installé dans la baie
Product Name (Nom du produit)	Nom descriptif commun de la lame de serveur
Part Number (Référence)	Numéro de référence à utiliser pour commander une lame de serveur supplémentaire ou de remplacement
System Board Spare Part Number (Référence de rechange de carte mère)	Référence à utiliser pour la commande d'une carte mère de remplacement de ce périphérique
Serial Number (Numéro de série)	Numéro de série unique de la lame de serveur
ROM Version (Version de ROM)	Numéro de version de la ROM


Device Bay Information - HP StorageWorks TapeBlade (Bay 6)
Status
Information
Virtual Devices
UID Light: Use the button below to toggle the state of the server's UID Light. Note: When the UID Light is in a blink state, a critic
being performed on the server and should not be interrupted.
Off
Toggle On/Off

Le voyant d'UID de la lame de stockage est activé/désactivé à partir de cet écran. Pour changer l'état du voyant d'UID de la lame, cliquez sur le bouton **Toggle On/Off** (Activer/Désactiver).

L'icône directement au-dessus du bouton Toggle On/Off est grisée lorsque le voyant d'UID de la lame est inactif et est bleu s'il est actif.

Informations de lame d'extension E/S

La sélection d'une lame d'extension E/S spécifique affiche la page Device Bay Information — Bay xx (Informations sur la baie de périphérique — Baie xx), où xx est la baie sélectionnée. Les informations présentées sur cet écran incluent des onglets concernant l'état, des informations et les périphériques virtuels.

Onglet Status

Informations d'état

Rangée	Description
Status (État)	État global de la lame. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Failed (Échec).
Powered (Alimentée)	État d'alimentation de la lame. Les valeurs possibles sont On (Activé) et Off (Désactivé).
Power Allocated (Puissance allouée)	Puissance d'alimentation autorisée pour la lame, en watts.
Partner Device (Périphérique partenaire)	La lame de serveur à laquelle est associée la lame d'extension E/S.
Virtual Fan (Ventilateur virtuel)	Pourcentage de la vitesse maximum (RPM) du ventilateur virtuel.

Les informations du tableau d'informations d'état correspondent au dernier téléchargement. Cliquez sur **Refresh** (Actualiser) pour actualiser les informations d'état.

Informations de diagnostics

Les informations de diagnostics sont recueillies de deux façons : Par interrogation du microcontrôleur de périphérique (résultat d'un état détérioré si une panne s'est produite) ou envoyées par le microcontrôleur du périphérique, sans interrogation, pour signaler une panne.

Rangée	Description
Device Identification Data (Données d'identification du périphérique)	Contient des informations telles que le nom du modèle, la référence, le numéro de série, ainsi que d'autres informations utilisées pour identifier le périphérique. Ces données sont également appelées données FRU. Une erreur de données d'identification du périphérique s'affiche si les données sont absentes ou illisibles par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Management Processor (Processeur de gestion)	État du iLO. Les valeurs possibles sont OK et Error.
I/O Configuration (Configuration E/S)	La configuration de la baie de périphérique est incorrecte. Si une lame de stockage est associée à une lame de serveur pleine hauteur, et que la lame de serveur ne dispose pas de la carte mezzanine appropriée, une configuration E/S non valide en résulte. Les valeurs possibles sont OK et I/O mismatch detected (Discordance E/S détectée).
Power Allocation Request (Demande d'allocation d'alimentation)	La puissance est insuffisante pour alimenter cette lame de serveur correctement. Les valeurs possibles sont OK et Insufficient enclosure power (Alimentation de boîtier insuffisante).
Cooling (Refroidissement)	Le nombre de ventilateurs est insuffisant pour ventiler correctement cette lame de serveur ou la configuration des

Rangée	Description
	ventilateurs est incorrecte. Les valeurs possibles sont OK et Insufficient fans for enclosure cooling (Nombre de ventilateurs insuffisant pour refroidissement du boîtier).
Device Location (Emplacement du périphérique)	La lame E/S n'a pas été placée dans le bon logement du boîtier d'après la configuration actuelle de ventilation. Les valeurs possibles sont OK et Incorrect location for proper device cooling (Emplacement incorrect pour refroidissement correct du périphérique).
Device Operational (Périphérique fonctionnel)	Le périphérique présente un défaut. L'état n'a pas été demandé par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Device Degraded (Périphérique détérioré)	Le périphérique présente un défaut. L'état a été demandé par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Partner Device Presence (Présence de périphérique partenaire)	La lame d'extension E/S a un serveur associé. Il doit s'agir d'un serveur placé à côté de celle-ci dans la configuration correcte. Les valeurs possibles sont OK et No adjacent partner found (Aucun partenaire adjacent trouvé).
Power Sequence (Séquence d'alimentation)	La lame d'extension E/S doit toujours être alimentée en premier. Si une lame d'extension E/S est insérée à côté d'une lame de serveur déjà alimentée, l'alimentation est refusée. La lame de serveur doit être mise hors tension afin que la lame d'extension E/S puisse être alimentée, puis la lame de serveur peut à nouveau être mise sous tension. Les valeurs possibles sont OK et Potential partner device is already ON (Partenaire potentiel déjà alimenté).
Partner Device Link (Lien du périphérique partenaire)	Les valeurs possibles sont OK et Inappropriate device in adjacent bay (Périphérique inapproprié dans baie adjacente). Ces informations ne s'affichent pas si la lame de serveur n'est pas associée à une lame de stockage/extension.

Capteurs de température

Colonne	Description
Sensor (Capteur)	Numéro du capteur
Location (Emplacement)	Emplacement du capteur dans le périphérique
Status (État)	État du capteur de température. L'état correspond à la présentation graphique de la température
Temperature (Température)	Présentation graphique de la température

Onglet de périphériques virtuels de lame d'extension E/S

UID Light (Voyant UID)

Un clic sur **Toggle On/Off** (Activer/Désactiver) allume (bleu) ou éteint (gris) le voyant d'UID sur la lame d'extension E/S afin d'identifier aisément la lame d'extension E/S sélectionnée.

Onglet d'informations de lame d'extension E/S

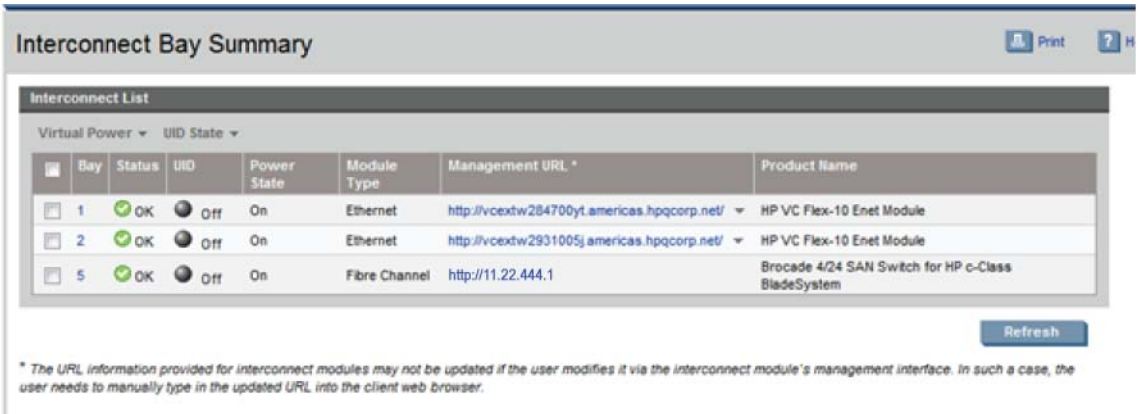
Informations sur le périphérique

Rangée	Description
Blade Type (Type de lame)	Lame d'extension E/S
Manufacturer (Fabricant)	Nom de la société qui a fabriqué la lame d'extension E/S
Product Name (Nom du produit)	Nom descriptif courant de la lame d'extension E/S
Part Number (Référence)	Numéro de référence à utiliser pour commander une lame d'extension E/S supplémentaire ou de remplacement de ce type
System Board Spare Part Number (Référence de rechange de carte mère)	Numéro de référence à utiliser pour commander une carte mère supplémentaire ou de remplacement de ce type
Serial Number (Numéro de série)	Numéro de série unique de la lame d'extension E/S
ROM Version (Version de ROM)	Numéro de version de la ROM

Baies d'interconnexion

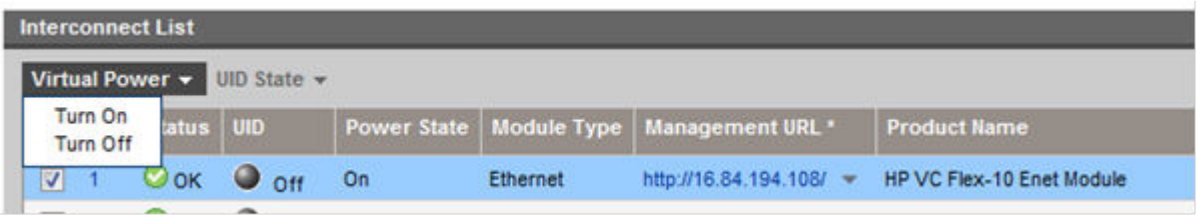
Écran Interconnect Bay Summary

Dans le menu Enclosure Information (Informations sur le boîtier), la catégorie Interconnect Bays (Baies d'interconnexion) répertorie tous les périphériques d'interconnexion dans le boîtier. La sélection de l'option de menu Interconnect Bays affiche directement la liste des périphériques d'interconnexion, avec une grille qui illustre l'état de chaque périphérique d'interconnexion dans le boîtier, ainsi que l'état de l'UID, l'état d'alimentation, le type de module, l'URL de gestion et le nom du produit. Ces paramètres sont décrits dans le tableau près de la fin de cette section.


Interconnect Bay Summary
Print
Interconnect List
Virtual Power
UID State
Bay
Status
UID
Power State
Module Type
Management URL *
Product Name
1 OK Off On Ethernet http://vcextw284700yt.americas.hpqcorp.net/ HP VC Flex-10 Enet Module
2 OK Off On Ethernet http://vcextw2931005j.americas.hpqcorp.net/ HP VC Flex-10 Enet Module
5 OK Off On Fibre Channel http://11.22.444.1 Brocade 4/24 SAN Switch for HP c-Class BladeSystem
Refresh
* The URL information provided for interconnect modules may not be updated if the user modifies it via the interconnect module's management interface. In such a case, the user needs to manually type in the updated URL into the client web browser.

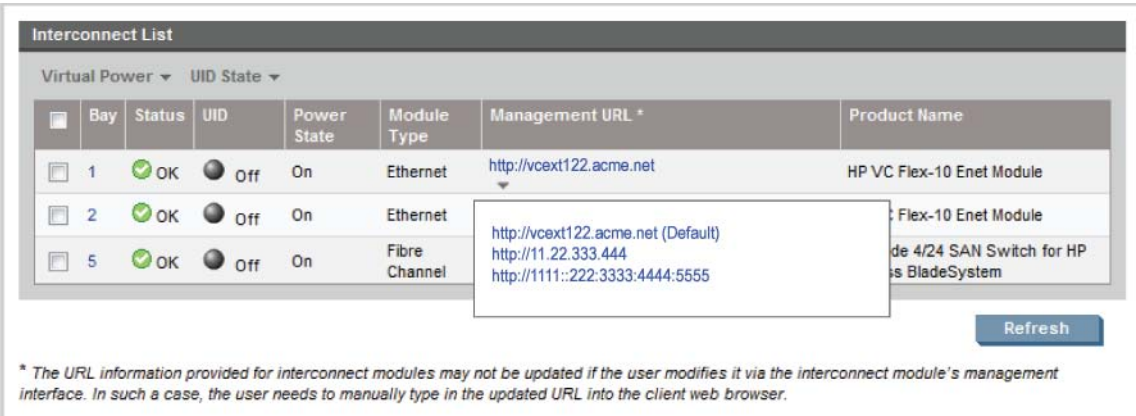
La case à cocher située dans la première colonne, sur la ligne du haut, permet d'activer/de désactiver simultanément toutes les cases à cocher de tous les périphériques d'interconnexion. Cette fonction est utile si, par exemple, vous souhaitez basculer l'état de l'UID pour tous les périphériques d'interconnexion au même moment. Sinon, la première colonne contient également des cases à cocher, que vous pouvez utiliser pour sélectionner des interconnexions individuellement. Une fois les interconnexions appropriées sélectionnées, vous pouvez utiliser le menu déroulant Virtual Power ou UID State (cliquez sur la flèche vers le bas correspondante) pour effectuer l'action appropriée.

Le menu Virtual Power illustrée dans la figure suivante permet d'activer ou de désactiver un périphérique d'interconnexion. HP vous recommande de n'activer ou désactiver qu'un seul périphérique à la fois à l'aide de cette fonction.



Le menu UID State (État de l'UID) illustré dans la figure suivante permet de définir l'état du voyant d'UID sur le périphérique d'interconnexion. L'activation du voyant d'UID permet de localiser plus facilement un périphérique d'interconnexion spécifique dans un boîtier. Vous pouvez activer ou désactiver ces voyants individuellement ou en groupes, selon les cases à cocher sélectionnées.

Pour afficher les liens d'adresse Management Console disponibles (IPv4 et IPv6), cliquez sur la flèche vers le bas le long de l'adresse Management Console. Une fenêtre contextuelle s'affiche, comme indiqué dans la figure suivante. Lorsque la prise en charge du lien FQDN est activée et que certaines exigences de configuration DNS sont remplies, une adresse basée sur le nom de domaine complet s'affiche en tant qu'URL de gestion par défaut (comme illustré). Pour plus d'informations sur l'activation de la prise en charge du lien FQDN, consultez la page « Accès réseau ».



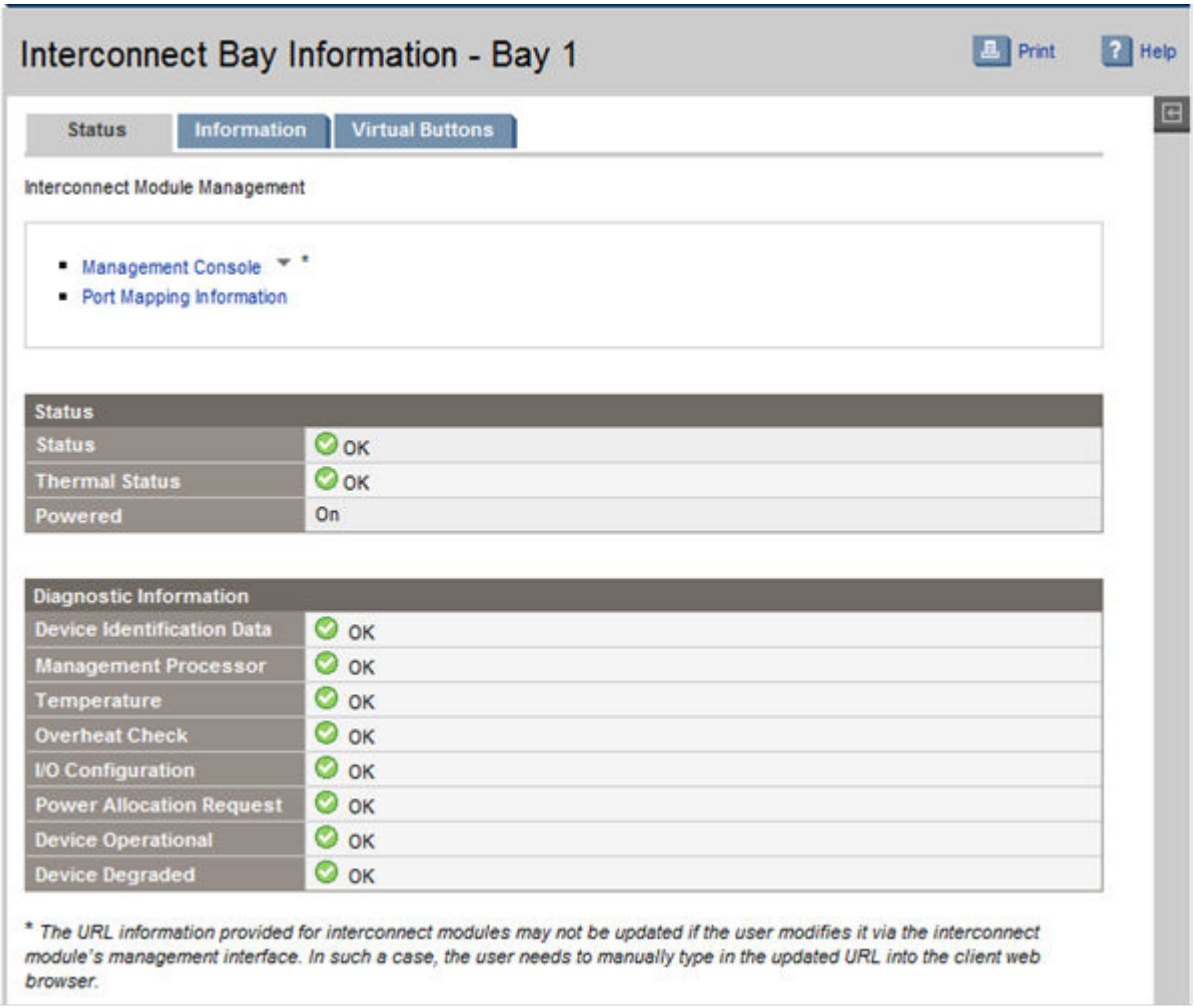
Colonne	Description
Case à cocher	Cochez les cases en regard de la ou des baies auxquelles appliquer les fonctions Virtual Power et UID State.
Bay (Baie)	Baie dans le boîtier du périphérique d'interconnexion correspondant. Ce champ affiche uniquement les baies peuplées. Les baies vides n'apparaissent pas dans ce tableau.
Status (État)	État global du périphérique d'interconnexion. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Failed (Échec).

Colonne	Description
UID	État de l'UID sur le périphérique d'interconnexion. Les valeurs possibles sont On (Activé, en bleu) et Off (Désactivé, en gris).
Power State (État de l'alimentation)	État d'alimentation du périphérique d'interconnexion. Les valeurs possibles sont On (Activé) et Off (Désactivé).
Module Type (Type de module)	Type d'interface réseau pour le périphérique d'interconnexion installé dans cette baie. Les valeurs possibles sont Ethernet et fibre.
Management URL (URL de gestion)	Adresse IPv4 à laquelle le périphérique d'interconnexion peut être géré et configuré pour une utilisation dans le réseau. Pour afficher les liens d'adresse URL de gestion disponibles (IPv4 et IPv6), cliquez sur la flèche vers le bas pour afficher un menu déroulant. Lorsque la prise en charge du lien FQDN est activée et que certaines exigences de configuration DNS sont remplies, une adresse basée sur le nom de domaine complet s'affiche en tant qu'URL de gestion par défaut. Pour plus d'informations sur l'activation de la prise en charge du lien FQDN, consultez la page « Accès réseau ».
Product Name (Nom du produit)	Nom descriptif courant du périphérique d'interconnexion.

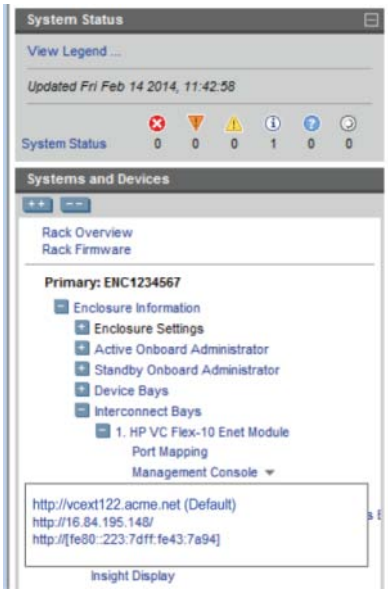
Les informations sur cette page sont actuelles à l'heure du dernier téléchargement. Pour visualiser des informations mises à jour, cliquez sur **Refresh** (Actualiser).

Écran Interconnect Bay

L'écran Interconnect Bay (Baie d'interconnexion) présente des informations sur les baies dans lesquelles des commutateurs et des routeurs peuvent être placés. Il affiche également les modules Onboard Administrator.



Pour vous connecter à la console de gestion, cliquez sur le lien **Management Console**. Pour afficher les liens disponibles d'adresses (IPv4 et IPv6) de la console de gestion, cliquez sur la flèche vers le bas à côté du lien. Vous pouvez également vous connecter à la console de gestion à partir de l'arborescence de navigation, comme indiqué dans la figure suivante. Dans les deux cas, lorsque la prise en charge du lien FQDN est activée et que certaines exigences de configuration DNS sont remplies, une adresse basée sur le nom de domaine complet s'affiche comme liaison par défaut. Pour plus d'informations sur l'activation de la prise en charge du lien FQDN, consultez la page « Accès réseau ».



Pour afficher des informations sur le mappage de ports de la baie d'interconnexion sélectionnée, cliquez sur le lien **Port MappingInterconnect**. Vous pouvez également sélectionner ces informations dans l'arborescence.

Informations d'état

Rangée	Description
Status (État)	État global du périphérique d'interconnexion. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Failed (Échec).
Thermal Status (État thermique)	État thermique du périphérique d'interconnexion. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Failed (Échec).
Powered (Alimentée)	État d'alimentation de la lame. Les valeurs possibles sont On (Activée), Off (Désactivée) et Delayed (Temporisée).
Power Delay Remaining (Délai restant avant alimentation)	Temps restant en secondes avant la mise sous tension du périphérique.

Informations de diagnostics

Rangée	Description
Device Identification Data (Données d'identification du périphérique)	Contient des informations telles que le nom du modèle, la référence, le numéro de série, ainsi que d'autres informations utilisées pour identifier le périphérique. Ces données sont également appelées données FRU. Une erreur de données d'identification du périphérique s'affiche si les données sont absentes ou illisibles par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Management Processor (Processeur de gestion)	Le processeur de supervision ne répond pas. Les valeurs possibles sont OK et Error.

Rangée	Description
Temperature (Température)	La température est au-dessus du seuil d'avertissement. Les valeurs possibles sont OK et Temperature Warning (Avertissement de température).
Overheat Check (Contrôle de surchauffe)	La température est au-dessus du seuil de danger. Les valeurs possibles sont OK et Critical temperature threshold reached (Seuil critique de température atteint).
I/O Configuration (Configuration E/S)	La configuration de la baie d'interconnexion est incorrecte. Les valeurs possibles sont OK et I/O mismatch (Discordance E/S).
Power Allocation Request (Demande d'allocation d'alimentation)	La puissance est insuffisante pour alimenter l'interconnexion correctement. Les valeurs possibles sont OK et Insufficient enclosure power (Alimentation de boîtier insuffisante).
Device Operational (Périphérique fonctionnel)	Échec du périphérique. L'état n'a pas été demandé par le Onboard Administrator. Les valeurs possibles sont OK et Error.
Device Degraded (Périphérique détérioré)	Échec du périphérique. L'état a été demandé par le Onboard Administrator. Les valeurs possibles sont OK et Error.
Device Informational (Informations relatives au périphérique)	Le périphérique fonctionne normalement mais réclame de l'attention.
Duplicate IP Address (Adresse IP dupliquée)	Coche pour vérifier si une adresse IP dupliquée existe sur le réseau au cours de l'attribution. Les valeurs possibles sont OK ou un message d'informations indiquant s'il existe une adresse IP dupliquée sur le réseau.

Onglet Interconnect Bay Information

Informations matérielles

Rangée	Description
Product Name (Nom du produit)	Nom descriptif commun du périphérique d'interconnexion.
Management IP Address (Adresse IP de gestion)	Adresse IP de l'interface de gestion d'interconnexion.
Management URL (URL de gestion)	Adresse à laquelle le périphérique d'interconnexion peut être géré et configuré pour une utilisation dans le réseau.
User Assigned Name (Nom affecté par l'utilisateur)	Nom affecté à l'interconnexion par l'utilisateur. Si pris en charge, le nom est affecté à l'aide de l'interface de gestion de l'interconnexion.
Part Number (Référence)	Référence à utiliser pour la commande d'un périphérique d'interconnexion supplémentaire de ce type.
Spare Part Number (Numéro de la pièce de rechange)	Référence à utiliser pour la commande d'un périphérique d'interconnexion de remplacement de ce type.
Serial Number (Numéro de série)	Numéro de série unique du périphérique d'interconnexion.
Type	Type d'interface du périphérique d'interconnexion. Les valeurs possibles sont Ethernet et fibre.
Manufacturer (Fabricant)	Nom de la société qui a fabriqué le périphérique d'interconnexion.

Rangée	Description
Temperature Sensor (Capteur de température)	Indique si le périphérique d'interconnexion comporte un capteur de température.
Firmware Version (Version du microprogramme)	Version de microprogramme du module d'interconnexion.
VLAN ID (Name) (ID VLAN [Nom])	Numéro d'ID VLAN et nom affectés à la baie d'interconnexion.

Informations IPv6

Rangée	Description
Link Local Address (Adresse locale du lien)	Adresse IPv6 locale du lien de l'interface d'interconnexion.
EBIPA Address (Adresse EBIPA)	Adresse IPv6 EBIPA de l'interface d'interconnexion.
Adresse DHCPv6	Adresse IPv6 DHCP de l'interface d'interconnexion
Adresse SLAAC	Adresse IPv6 SLAAC de l'interface d'interconnexion.
Link Local Management URL (URL de gestion locale du lien)	URL de gestion IPv6 locale du lien à laquelle le périphérique d'interconnexion peut être géré et configuré pour une utilisation dans le réseau.
EBIPA to Management URL (URL de gestion EBIPA)	URL de gestion IPv6 EBIPA à laquelle le périphérique d'interconnexion peut être géré et configuré pour une utilisation dans le réseau.
DHCP IPv6 Management URL (URL de gestion IPv6 DHCP)	URL de gestion IPv6 DHCP à laquelle le périphérique d'interconnexion peut être géré et configuré pour une utilisation dans le réseau.
SLAAC Management URL (URL de gestion SLAAC)	URL de gestion IPv6 SLAAC à laquelle le périphérique d'interconnexion peut être géré et configuré pour une utilisation dans le réseau.

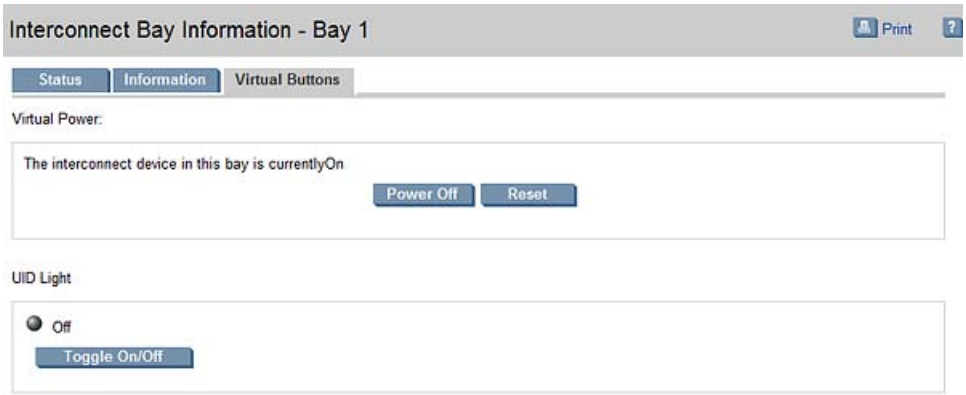
Informations de connectivité

Rangée	Description
JS2 Connector (Connecteur JS2)	Ce champ indique la présence ou l'absence du connecteur JS2.
Internal Ethernet Interface to OA (Interface Ethernet interne vers OA)	Ce champ indique la présence ou l'absence d'une interface Ethernet interne vers le module Onboard Administrator.
Internal Ethernet Route to OA (Itinéraire Ethernet interne vers OA)	Ce champ indique l'état d'un itinéraire Ethernet interne vers le module Onboard Administrator. Les valeurs possibles sont Enabled (Activé) et Disabled (Désactivé).
Internal Serial Interface to OA (Interface série interne vers OA)	Ce champ indique la présence ou l'absence d'une interface série interne vers le module Onboard Administrator.
Internal Serial Route to OA (Itinéraire série interne vers OA)	Ce champ indique l'état d'un itinéraire série interne vers le module Onboard Administrator. Les valeurs possibles sont Enabled (Activé) et Disabled (Désactivé).
Serial Port Baud Rate (Débit en bauds du port série)	Ce champ affiche le débit en bauds du port série.

Rangée	Description
External Serial Port Interface (Interface de port série externe)	Ce champ indique la présence ou l'absence d'une interface de port série externe.
External Ethernet Interface (Interface Ethernet externe)	Ce champ indique la présence ou l'absence d'une interface Ethernet externe.

Boutons virtuels de la baie d'interconnexion

Les boutons virtuels de la baie d'interconnexion permettent de remettre sous ou hors tension, de réinitialiser, ou d'activer/désactiver l'UID du périphérique souhaité depuis l'interface utilisateur du module Onboard Administrator.

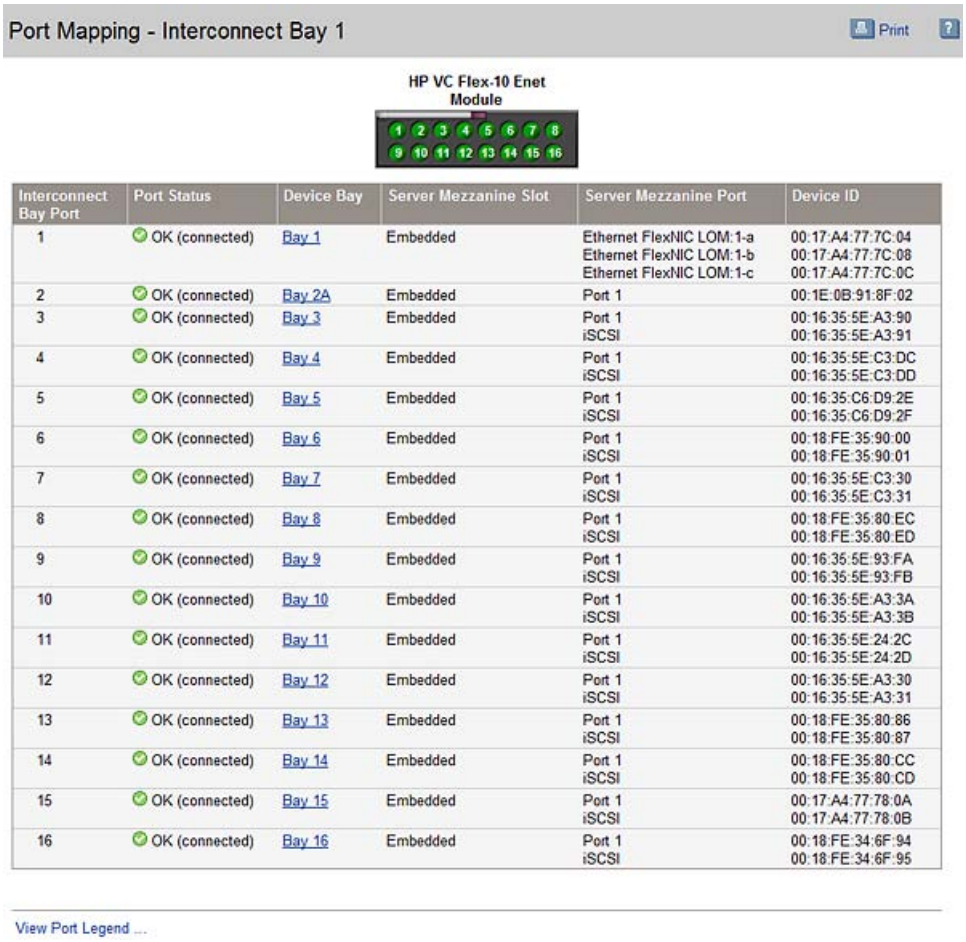


Bouton	Description
Power Off (Mettre hors tension)	Met le périphérique d'interconnexion hors tension.
Reset (Réinitialiser)	Force le périphérique d'interconnexion à s'arrêter, puis à redémarrer, c'est-à-dire à exécuter une réinitialisation.
Toggle On/Off (Activer/Désactiver)	Active (bleu) ou désactive (gris) l'UID du périphérique d'interconnexion pour faciliter l'identification du périphérique d'interconnexion sélectionné.

REMARQUE : Si un module d'interconnexion est mis hors tension, le module sera mis sous tension une fois qu'un module Onboard Administrator redémarre ou que le module bascule si une alimentation suffisante de boîtier est disponible.

Écran Interconnect Bay Port Mapping

L'écran Interconnect Bay Port Mapping (Mappage des ports de la baie d'interconnexion) présente une vue graphique et une vue sous forme de tableau du mappage des ports de la baie d'interconnexion.


Port Mapping - Interconnect Bay 1
Print
HP VC Flex-10 Enet Module
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
Interconnect Bay Port
Port Status
Device Bay
Server Mezzanine Slot
Server Mezzanine Port
Device ID
1 OK (connected) Bay 1 Embedded Ethernet FlexNIC LOM:1-a Ethernet FlexNIC LOM:1-b Ethernet FlexNIC LOM:1-c 00:17:A4:77:7C:04 00:17:A4:77:7C:08 00:17:A4:77:7C:0C
2 OK (connected) Bay 2A Embedded Port 1 00:1E:0B:91:8F:02
3 OK (connected) Bay 3 Embedded Port 1 iSCSI 00:16:35:5E:A3:90 00:16:35:5E:A3:91
4 OK (connected) Bay 4 Embedded Port 1 iSCSI 00:16:35:5E:C3:DC 00:16:35:5E:C3:DD
5 OK (connected) Bay 5 Embedded Port 1 iSCSI 00:16:35:C6:D9:2E 00:16:35:C6:D9:2F
6 OK (connected) Bay 6 Embedded Port 1 iSCSI 00:18:FE:35:90:00 00:18:FE:35:90:01
7 OK (connected) Bay 7 Embedded Port 1 iSCSI 00:16:35:5E:C3:30 00:16:35:5E:C3:31
8 OK (connected) Bay 8 Embedded Port 1 iSCSI 00:18:FE:35:80:EC 00:18:FE:35:80:ED
9 OK (connected) Bay 9 Embedded Port 1 iSCSI 00:16:35:5E:93:FA 00:16:35:5E:93:FB
10 OK (connected) Bay 10 Embedded Port 1 iSCSI 00:16:35:5E:A3:3A 00:16:35:5E:A3:3B
11 OK (connected) Bay 11 Embedded Port 1 iSCSI 00:16:35:5E:24:2C 00:16:35:5E:24:2D
12 OK (connected) Bay 12 Embedded Port 1 iSCSI 00:16:35:5E:A3:30 00:16:35:5E:A3:31
13 OK (connected) Bay 13 Embedded Port 1 iSCSI 00:18:FE:35:80:86 00:18:FE:35:80:87
14 OK (connected) Bay 14 Embedded Port 1 iSCSI 00:18:FE:35:80:CC 00:18:FE:35:80:CD
15 OK (connected) Bay 15 Embedded Port 1 iSCSI 00:17:A4:77:78:0A 00:17:A4:77:78:0B
16 OK (connected) Bay 16 Embedded Port 1 iSCSI 00:18:FE:34:6F:94 00:18:FE:34:6F:95
View Port Legend ...

Vue graphique

Lorsque vous déplacez la souris au-dessus du port de la baie d'interconnexion, la vue graphique présente les mêmes informations que celles affichées dans la vue sous forme de tableau.

Vue sous forme de tableau

Colonne	Description
Interconnect Bay Port (Port de la baie d'interconnexion)	Numéro de la baie d'interconnexion, compris entre 1 et 16
Port Status (État du port)	État courant du port
Device Bay (Baie de périphérique)	Baie de périphérique correspondant au mappage des ports d'interconnexion
Server Mezzanine Slot (Connecteur de mezzanine du serveur)	Type de périphérique placé dans la mezzanine de la lame de serveur
Server Mezzanine Port (Port de mezzanine du serveur)	Port physique du périphérique mezzanine
Device ID (ID du périphérique)	Adresse MAC du port de la baie d'interconnexion

Gestion de l'alimentation de boîtier

Planification de la gestion de l'alimentation

Chaque boîtier d'alimentation contient six alimentations contrôlées directement par Onboard Administrator. Vous pouvez brancher jusqu'à deux boîtiers d'alimentation à un seul et même boîtier.

Onboard Administrator calcule l'état de redondance, la puissance disponible totale et la puissance totale consommée. Ces informations sont affichées à l'attention de l'utilisateur et permettent de gérer les ressources d'alimentation. Les écrans du sous-système d'alimentation du module Onboard Administrator présentent l'état de chaque alimentation et des informations sur chacune d'elles, de même que sur le boîtier d'alimentation lui-même.

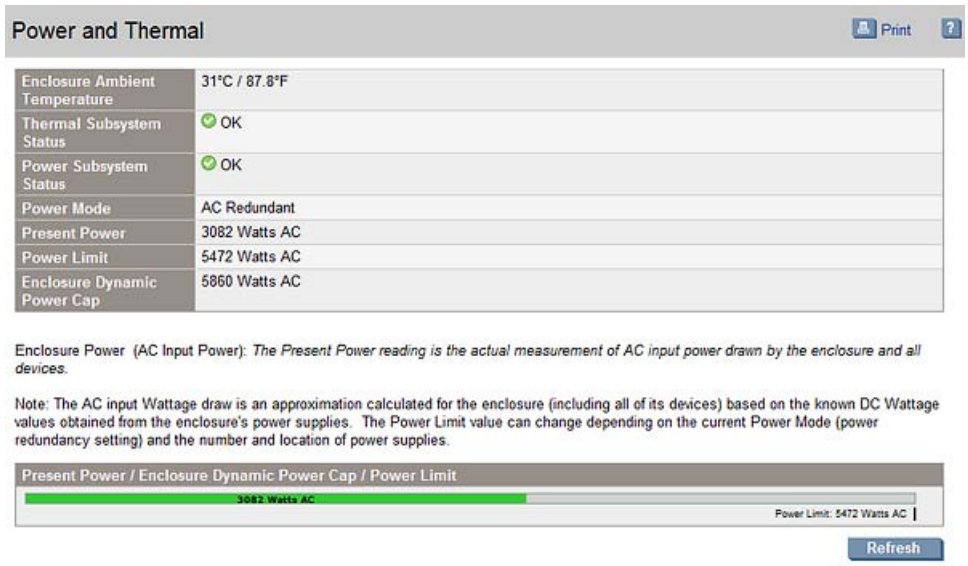
L'espace d'erreur d'alimentation inclut également les fusibles électroniques situés entre le fond de panier d'alimentation et les baies de serveur ou les travées. Onboard Administrator vous alertera des déclenchements de fusibles afin de pouvoir les réinitialiser manuellement.

Lors de l'installation d'alimentations supplémentaires dans le boîtier, notez que l'utilisation de références d'alimentation différentes dans le même boîtier n'est pas prise en charge. Le module Onboard Administrator vous signale quelles alimentations doivent être remplacées en affichant une icône d'avertissement.

REMARQUE : Les alimentations HP 1200W Common Slot Silver Hot Plug, références de rechange 441830-001 et 498152-001, peuvent être combinées dans un boîtier et sont traitées comme équivalentes, à des fins de mélange de blocs d'alimentation.

Pour installer correctement les alimentations dans le boîtier, consultez le Manuel d'installation et de configuration du boîtier HP BladeSystem c7000.

Écran Power and Thermal


Power and Thermal
Print
Enclosure Ambient Temperature
31°C / 87.8°F
Thermal Subsystem Status
OK
Power Subsystem Status
OK
Power Mode
AC Redundant
Present Power
3082 Watts AC
Power Limit
5472 Watts AC
Enclosure Dynamic Power Cap
5860 Watts AC
Enclosure Power (AC Input Power): The Present Power reading is the actual measurement of AC input power drawn by the enclosure and all devices.
Note: The AC input Wattage draw is an approximation calculated for the enclosure (including all of its devices) based on the known DC Wattage values obtained from the enclosure's power supplies. The Power Limit value can change depending on the current Power Mode (power redundancy setting) and the number and location of power supplies.
Present Power / Enclosure Dynamic Power Cap / Power Limit
3082 Watts AC
Power Limit: 5472 Watts AC
Refresh

Rangée	Description
Enclosure Ambient Temperature (Température ambiante du boîtier)	Ce champ affiche la température ambiante la plus élevée reportée par les périphériques de lame installés. Si aucun périphérique de lame n'est installé, ce champ affiche la

Rangée	Description
	température du module Onboard Administrator en tant qu'approximation de la température ambiante.
Thermal Subsystem Status (État thermique du sous-système)	État thermique global du boîtier. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Critical Error (Erreur critique).
Power Subsystem Status (État de l'alimentation du sous-système)	État de l'alimentation globale du boîtier. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Critical Error (Erreur critique).
Power Mode (Mode d'alimentation)	Paramètre utilisateur destiné à configurer la capacité de puissance CC du boîtier et le mode de redondance d'entrée du boîtier. Voir la section « Gestion de l'alimentation » pour connaître les valeurs possibles.
Present Power (Puissance actuelle)	Quantité de puissance en watts consommée par tous les périphériques dans le boîtier.
Power Limit (Limite de puissance)	Puissance d'alimentation disponible pour la consommation du boîtier, mesurée en watts.
Enclosure Dynamic Power Cap (Limitation dynamique de la puissance du boîtier)	Une limite d'alimentation sur un groupe de serveurs dans le boîtier. Lorsque les serveurs fonctionnent, la demande en puissance varie en fonction de chaque serveur. Une limite de puissance est définie pour chaque serveur. Elle est suffisante pour lui permettre de faire face à sa charge de travail, mais reste conforme à la limitation dynamique de la puissance du boîtier. La surveillance continue des demandes d'alimentation et les ajustements automatiques des limites d'alimentation du serveur assurent une dégradation minimale des performances. Les informations de limitation d'alimentation dynamique du boîtier apparaissent uniquement si une limitation a été définie.

Present Power/Enclosure Dynamic Power Cap/Power Limit (Alimentation présente/Limitation d'alimentation dynamique de boîtier/Limite d'alimentation)

La valeur Present Power (Alimentation présente) représente la puissance en watts consommée par tous les périphériques du boîtier. La limitation d'alimentation dynamique du boîtier ajuste automatiquement les limites d'alimentation sur les serveurs dans le boîtier pour répondre aux demandes de charge sur les serveurs tout en se conformant à la limitation d'alimentation dynamique du boîtier. La limite d'alimentation est le montant maximum de puissance d'entrée disponible pour une consommation par le boîtier. La limite d'alimentation est dépendante du paramètre de redondance de puissance du boîtier et du nombre et de l'emplacement des alimentations dans le boîtier. Si une limite d'alimentation statique a été spécifiée, la limite d'alimentation affiche cette limite.

Gestion de l'alimentation

Pour définir les options de gestion de l'alimentation dans Onboard Administrator, accédez au menu sur la gauche et sélectionnez le boîtier à gérer. Cliquez sur **Power and Thermal>Power Management** (Alimentation et température>Gestion de l'alimentation). La page principale Power Management (Gestion de l'alimentation) s'affiche et propose les choix suivants :

- AC Redundant (Redondance secteur)
- Power Supply Redundant (Redondance d'alimentation)
- Not DC Redundant (Pas de redondance CC)

Située sous les choix de gestion d'alimentation principale, la case à cocher Enable Dynamic Power permet d'activer ou de désactiver le mode d'alimentation dynamique.

Le champ Limit AC Input VA (Limitation des VA d'alimentation CA) permet de définir un nombre limite de VA pour le boîtier. Lorsque le boîtier atteint cette limite, il interdit la mise sous tension de toute lame, de toute alimentation, de tout ventilateur ou de tout commutateur supplémentaire. Si une valeur inférieure au nombre de VA actuellement utilisé pour le boîtier est entrée dans le champ de limitation des VA, le boîtier ne mettra hors tension aucun périphérique contenu dans le boîtier. Toutefois, si un périphérique est mis hors tension, il ne peut pas être mis sous tension en raison de la règle de limitation des VA définie dans les paramètres de gestion d'alimentation du module Onboard Administrator.

REMARQUE : Si le mode de redondance est DC Redundant, AC Redundant ou Power Supply Redundant et que la redondance d'alimentation est perdue, vous devez ajouter des alimentations supplémentaires ou modifier le paramètre du mode de redondance dans le module Onboard Administrator pour restaurer l'état du sous-système d'alimentation. Consultez l'écran Insight Display pour connaître les mesures correctives.

REMARQUE : Pour modifier le mode de redondance d'alimentation, vous devez désactiver EDPC. Une fois le mode de redondance d'alimentation modifié, réinitialisez EDPC sur la base des nouvelles plages.

Options de gestion de l'alimentation

Le système de gestion d'alimentation du boîtier HP BladeSystem c3000 ou c7000 vous permet de configurer le boîtier selon vos besoins. Vous pouvez choisir parmi les options de gestion d'alimentation dans l'écran Onboard Administrator Power Management. Ces options de gestion d'alimentation sont décrites dans le tableau suivant.

Option de gestion de l'alimentation	Nom Insight Display	Description
Mode d'alimentation (mode de redondance d'alimentation)		
DC Redundant (redondance CC) ou AC Redundant (redondance CA)	DC Redundant (redondance CC) ou AC Redundant (redondance CA)	Le module OA détecte le type des blocs d'alimentation présents, adapte automatiquement le comportement du mode d'alimentation en conséquence et affiche le nom du mode correspondant : • Si des modules d'alimentation CC sont présents : mode de redondance CC • Si des modules d'alimentation CA sont présents : mode Redondant CA Également connu sous le nom redondance N+N ou redondance de grille. Les blocs d'alimentation *N* sont utilisés pour fournir l'alimentation et les blocs *N* sont utilisés pour fournir la redondance (où la valeur de *N* peut être 1, 2 ou 3). Jusqu'à trois alimentations peuvent s'avérer défectueuses sans entraîner de panne du boîtier. Lorsque le système est correctement câblé et comporte des lignes d'alimentation CC ou CA redondantes, cette

Option de gestion de l'alimentation	Nom Insight Display	Description
		configuration garantit que la panne d'une ligne d'alimentation CC ou CA n'entraîne pas la mise hors tension du boîtier. Au cas, peu probable, où la batterie de secours ne parvient pas à fournir l'alimentation en raison de plusieurs défaillances de bloc d'alimentation ou d'une panne du réseau électrique, le système peut être mis hors tension. Le système se met hors tension lorsque les blocs d'alimentation restants ne fournissent pas une alimentation suffisante pour répondre aux exigences d'alimentation du système. Les modes de redondance CA ou CC requièrent au moins deux blocs d'alimentation. Quel que soit le mode, HP recommande d'utiliser un nombre pair de blocs d'alimentation (2, 4 ou 6). Dans ce cas, *N* blocs d'alimentation servent à l'alimentation et *N* autres servent à assurer la redondance (où *N* est égal à 1, 2 ou 3). Si vous utilisez un nombre impair de blocs d'alimentation (3 ou 5), *N* sont utilisés pour fournir l'alimentation et N + 1 sont utilisés pour la redondance (où *N* est égal à 1 ou 2). Le mode de redondance CA ou CC protège également un système contre une panne du réseau électrique par l'utilisation d'un mode d'alimentation électrique de redondance CA ou CC (si correctement câblé). En mode de redondance CA, si vous utilisez un module d'entrée d'alimentation triphasée de boîtier c7000, HP recommande 6 blocs d'alimentation actifs (3+3) pour un équilibrage de phases correct.
Power Supply Redundant (Redondance d'alimentation)	Power Supply (Alimentation)	Pour tous les blocs d'alimentation. Ce mode prend en charge de deux à six blocs d'alimentation. Également appelé redondance N+1. Avec ce mode d'alimentation, *N* blocs d'alimentation servent à fournir l'alimentation et 1 est utilisé pour fournir la redondance (où la valeur *N* peut être 1, 2, 3, 4 ou 5). Si vous utilisez un module d'entrée d'alimentation triphasée de boîtier c7000, HP recommande 3 ou 6 blocs d'alimentation actifs (2+1 ou 5+1) pour un équilibrage de phases correct.

Option de gestion de l'alimentation	Nom Insight Display	Description
		Ce mode d'alimentation est conçu pour protéger le système en cas de panne de module d'alimentation. Dans le cas peu probable que plus d'un bloc d'alimentation ne parvient pas à fournir l'alimentation en raison de blocs d'alimentation défaillants ou d'une panne de grille d'alimentation, le système peut se mettre hors tension. Le système se met hors tension lorsque les blocs d'alimentation restants ne fournissent pas une alimentation suffisante pour répondre aux exigences d'alimentation du système.
Not Redundant (Non redondant)	Aucun	Pour tous les blocs d'alimentation. Ce mode prend en charge 1 à 6 blocs d'alimentation. Avec ce mode d'alimentation, *N* blocs d'alimentation servent à fournir l'alimentation et aucun n'est utilisé pour fournir la redondance (où la valeur *N* peut être 1, 2, 3, 4, 5 ou 6). Si vous utilisez un module d'entrée d'alimentation triphasée de boîtier c7000, HP recommande 3 ou 6 blocs d'alimentation actifs pour un équilibrage de phases correct Il n'existe pas de redondance d'alimentation et aucun avertissement de redondance d'alimentation n'est fourni. Si un bloc d'alimentation ne parvient pas à fournir l'alimentation en raison de blocs d'alimentation défaillants ou d'une panne de grille d'alimentation, le système peut se mettre hors tension. Il se mettra hors tension si les blocs d'alimentation restants ne disposent pas d'alimentation suffisante pour répondre aux exigences d'alimentation du système. Ce mode d'alimentation n'est pas recommandé pour les systèmes déployés dans des environnements de production.
Mode Alimentation dynamique (activé ou désactivé)		
Dynamic Power	Dynamic Power	S'il est activé, le mode d'alimentation dynamique place les alimentations inutilisées en mode Standby afin d'accroître l'efficacité de l'alimentation du boîtier et de réduire la consommation électrique du boîtier pendant les demandes plus faibles d'alimentation. L'augmentation de la demande en alimentation entraîne automatiquement le passage en mode pleinement opérationnel des alimentations en attente. Ce tableau est suivi d'informations supplémentaires sur l'alimentation dynamique.

Option de gestion de l'alimentation	Nom Insight Display	Description
Mode Limite de puissance		
Enclosure Dynamic Power Cap (Limitation dynamique de la puissance du boîtier)	Aucun	Permet de spécifier une limite pour la consommation électrique du boîtier. Le tirage de puissance est limité par la gestion dynamique des limitations d'alimentation des lames de serveur afin de rester sous la limitation d'alimentation globale du boîtier. Pour plus d'informations, consultez le tableau de limite de puissance qui suit.
Static Power Limit (Limite de puissance statique)	Power Limit (Limite de puissance)	Paramètre facultatif de limitation de la puissance. Chaque fois que vous essayez de mettre sous tension un périphérique, les demandes de puissance totale du nouveau périphérique et des périphériques déjà sous tension sont comparées à cette limite de puissance statique. Si les demandes de puissance totale dépassent la limite, la mise sous tension du nouveau périphérique est refusée. Pour plus d'informations sur la limite de puissance statique et la manière dont elle est comparée au plafond d'alimentation dynamique de boîtier, consultez le tableau de limite d'alimentation qui suit.

REMARQUE : Quel que soit le mode de redondance activé, tous les blocs d'alimentation fonctionnels présents dans le boîtier sont généralement actifs et partagent la prestation des besoins en alimentation du boîtier. Si le mode Alimentation dynamique est activé, certains blocs d'alimentation peuvent être placés automatiquement en veille pour augmenter l'efficacité globale de l'alimentation du boîtier. Pour plus d'informations, consultez la discussion relative au mode Alimentation dynamique qui suit.

Le module Onboard Administrator permet de modifier le paramètre de mode d'alimentation (redondance) après la mise sous tension du boîtier et des périphériques. Si le mode d'alimentation est modifié, le module Onboard Administrator actualise l'état de redondance en fonction des besoins, en signalant une redondance dégradée/défectueuse le cas échéant. Par exemple, le mode d'alimentation d'origine était Alimentation redondante (N+1) lorsque toutes les lames ont été mises sous tension, puis a été modifié sur Redondant CA (N+N), réduisant ainsi la capacité de puissance telle que vue par le module Onboard Administrator. Tant qu'une puissance suffisante est disponible, toutes les lames resteront opérationnelles. Toutefois, dans certaines circonstances, une lame ne se mettra pas sous tension, par exemple lorsque qu'elle remplace une autre lame de serveur. Des informations supplémentaires sont fournies dans le tableau et les sections qui suivent.

Dynamic Power (Alimentation dynamique) : le paramètre par défaut est Disabled (Désactivé). Les sélections suivantes sont valides :

- Enabled (Activé) : certaines alimentations peuvent être automatiquement placées en veille pour augmenter l'efficacité globale du sous-système d'alimentation du boîtier.
- Disabled (Désactivé) : toutes les alimentations partagent la charge. L'efficacité du sous-système d'alimentation varie en fonction de la charge.

REMARQUE : L'alimentation dynamique est prise en charge avec tous les blocs d'alimentation c3000. Elle est prise en charge avec tous les blocs d'alimentation c7000, à l'exception de ceux fonctionnant avec une tension d'entrée basse (nominale 100-120 VCA).

REMARQUE : Pour OA v4.01 et versions ultérieures, la valeur usine par défaut associée au paramètre Dynamic Power a été modifiée d'activée à désactivée. L'efficacité de fonctionnement des blocs d'alimentation de boîtiers HP Gold (rendement de 92 %) et HP Platinum (rendement de 94 %) actuellement disponible rend inutile cette stratégie de gestion de l'alimentation basée sur le microprogramme. Le paramètre Dynamic Power est recommandé uniquement pour les blocs d'alimentation de boîtier HP ayant une valeur de rendement inférieure à 92 %. Lors de la mise à niveau à OA v4.01 ou version ultérieure, le paramètre Dynamic Power actuel est conservé après la mise à niveau. Pour plus d'informations, consultez l'avis à la clientèle c03957955 (http://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03957955).

Power Limit (Limite de puissance)

Ne définissez pas de limite de puissance statique ou de plafond d'alimentation dynamique de boîtier sur un boîtier vide.

Mode	Nom Insight Display	Description
Enclosure Dynamic Power Cap (Limitation dynamique de la puissance du boîtier)	Aucun	Une fonctionnalité facultative qui permet de limiter les serveurs dans un boîtier en tant que groupe. Lorsque les serveurs fonctionnent, la demande en puissance varie en fonction de chaque serveur. Un plafond d'alimentation est configuré pour chaque serveur de manière à ce qu'il dispose de suffisamment de puissance pour répondre aux exigences de sa charge de travail tout en tenant compte du plafond d'alimentation dynamique du boîtier. Une carte OA redondante est requise pour paramétrer la fonction Dynamic Power Cap (Plafond d'alimentation dynamique). La fonction est activée avec trois paramètres de configuration : • Dynamic Power Cap (Plafond d'alimentation dynamique) : la consommation électrique moyenne totale du boîtier ne dépassera pas le plafond d'alimentation dynamique. • Derated Circuit Capacity (Capacité réduite du circuit) : la consommation électrique moyenne sur un circuit unique ne dépassera pas la capacité réduite du circuit. • Rated Circuit Capacity (Capacité nominale du circuit) : la consommation électrique de pointe sur un circuit unique ne dépassera pas la capacité nominale du circuit.

Mode	Nom Insight Display	Description
		Lors de la configuration de ces paramètres, le déclassement de puissance du circuit doit être au moins aussi élevé que le plafond de puissance dynamique et non supérieur à la capacité nominale du circuit. Le plafond d'alimentation dynamique est utilisé pour limiter la consommation électrique du boîtier sur la base d'une contrainte de refroidissement qui peut être inférieure à la capacité réduite du circuit. La capacité réduite du circuit est utilisée pour limiter la consommation électrique moyenne du boîtier sur un circuit. La capacité nominale du circuit est utilisée pour limiter la consommation électrique de pointe du boîtier sur un circuit. Si vous devez limiter la charge électrique ou la sortie thermique d'un boîtier, la méthode de plafond d'alimentation dynamique du boîtier est meilleure qu'une limite d'alimentation statique. Enclosure Dynamic Power Cap permet d'alimenter plus de lames que sur une limite d'alimentation statique.
Static Power Limit (Limite de puissance statique)	Power Limit (Limite de puissance)	Paramètre facultatif de limitation de la puissance. Chaque fois que vous essayez de mettre sous tension un périphérique, les demandes de puissance totale du nouveau périphérique et des périphériques déjà sous tension sont comparées à cette limite de puissance statique. Si les demandes de puissance totale dépassent la limite, la mise sous tension du nouveau périphérique est refusée. Une limite d'alimentation statique est meilleure lorsque : • Vous ne souhaitez imposer à vos lames des plafonds ajustés de manière dynamique. • Vous préférez ne pas alimenter une lame de serveur s'il est impossible de lui attribuer la pleine puissance (même si elle consomme typiquement moins). • Plus d'1/4 des lames du boîtier ne satisfont pas aux exigences définies pour le matériel ou le microprogramme eu égard au

Mode	Nom Insight Display	Description
		plafond d'alimentation dynamique du boîtier.
Aucun	Aucun	La consommation d'énergie du boîtier n'est pas supervisée ou plafonnée.

Différences entre plafond d'alimentation, plafond d'alimentation dynamique et plafond d'alimentation dynamique du boîtier

HP offre trois variétés de gestion de l'alimentation qui permettent aux utilisateurs de limiter la consommation d'énergie du serveur. Les trois variétés de plafonnement de l'alimentation fonctionnent pour limiter la consommation suivant un objectif en watts ou Btu/hr spécifié. Les trois technologies sont Plafond d'alimentation, Plafond d'alimentation dynamique et Plafond d'alimentation dynamique du boîtier.

Plafond d'alimentation

En mai 2007, HP a lancé la technologie de plafond d'alimentation avec la version 1.30 d'iLO 2. Cette technologie basée sur le microprogramme limite la consommation moyenne du serveur à une valeur en watts ou Btu/hr définie par l'utilisateur. Dans la mesure où cette technologie fonctionne dans le microprogramme, elle ne peut pas limiter la consommation d'alimentation assez rapidement pour assurer la protection des disjoncteurs au niveau des unités PDU. Le plafond d'alimentation limitant la consommation électrique assez rapidement pour protéger l'infrastructure de refroidissement, ceci est donc une solution efficace pour les centres de données faisant face à des contraintes de capacité de refroidissement. Le plafond d'alimentation est pris en charge sur tout serveur ou lame ProLiant doté d'un processeur de supervision iLO et de possibilités de mesure de puissance. L'utilisation du plafond d'alimentation requiert un microprogramme iLO 2 version 1.30 (ou ultérieure) et d'une paire ROM/BIOS système mise à jour.

Plafond dynamique de puissance

Le plafond dynamique de puissance est une technologie basée sur le matériel qui limite la consommation de puissance suffisamment rapidement pour protéger les disjoncteurs et l'infrastructure de refroidissement. En décembre 2008, HP a lancé la technologie de plafond dynamique d'alimentation avec la version 1.70 d'iLO 2. Les serveurs pris en charge contiennent un circuit matériel interne qui surveille la consommation d'énergie du serveur sur une base sous-secondaire. Si la consommation d'énergie du serveur s'approche de la limite de plafond d'alimentation définie dans iLO, le circuit matériel interne limite la consommation électrique suffisamment rapidement pour protéger les circuits au niveau de l'unité PDU d'un dépassement de souscription et empêcher les pannes de serveur liées à l'alimentation.

Le plafond dynamique d'alimentation requiert un matériel spécifique sur la carte mère. Le plafond dynamique d'alimentation requiert également le microprogramme iLO 2 version 1.70 (ou ultérieure) et un système ROM/BIOS daté du 01/10/2008 (ou ultérieure). iLO met automatiquement à jour le microprogramme dans le circuit matériel d'alimentation du plafond d'alimentation dynamique.

La limitation dynamique de la puissance du boîtier est prise en charge sur les lames de serveur BladeSystem suivantes :

- BL260c G5 (Remarques : 2)
- BL2x220 G5 (Remarques : 2)
- BL460c G1 (Remarques : 1 et 2)
- BL460c G5 (Remarques : 2)

- BL465c G5 (Remarques : 2)
- BL495c G5 (Remarques : 2)
- BL685c G5 (Remarques : 2)
- Toutes les lames de serveur G6
- Toutes les lames de serveur G7
- Toutes les lames de serveur G8

Informations complémentaires

- Ces systèmes nécessitent des cartes mère compatibles Quatre cœurs pour prendre en charge la limitation dynamique de la puissance.
- Lors de la mise en œuvre de la limitation de puissance pour HP BladeSystem, HP recommande d'utiliser la limitation dynamique de la puissance de boîtier définie dans l'ensemble du module Onboard Administrator. Pour utiliser la limitation dynamique de la puissance de boîtier, vous devez mettre à niveau le microprogramme iLO 2 à la version 1.70 ou ultérieure et vous êtes encouragé à mettre à jour la ROM système à la version 10/1/2008 ou ultérieure. Pour certains serveurs BL460c plus anciens, le microprogramme iLO peut ne pas pouvoir mettre à jour automatiquement le circuit matériel de limitation dynamique de la puissance. Dans ce cas, le module Onboard Administrator compense l'absence du circuit matériel interne et continue de garantir la protection du circuit.

Enclosure Dynamic Power Capping (Plafond d'alimentation dynamique du boîtier)

Enclosure Dynamic Power Capping combine la technologie de plafond dynamique d'alimentation du serveur BladeSystem avec un algorithme de contrôle d'équilibrage de l'alimentation dans le module Onboard Administrator afin de maximiser le rendement global du boîtier. Enclosure Dynamic Power Capping protège vos disjoncteurs et maximise votre rendement.

À l'aide du plafond d'alimentation dynamique du boîtier, vous définissez un plafond d'alimentation pour l'ensemble du boîtier. Le module Onboard Administrator alloue des limites individuelles à chaque lame de serveur participante. Les lames de serveur gèrent leur consommation suivant cette limite. Le module Onboard Administrator surveille continuellement les exigences de consommation pour chaque lame de serveur et rééquilibre en permanence les limites individuelles afin de veiller à ce que les lames de serveur occupées reçoivent plus de puissance que les lames de serveur inactives. Cette allocation d'alimentation améliore les performances globales du boîtier.

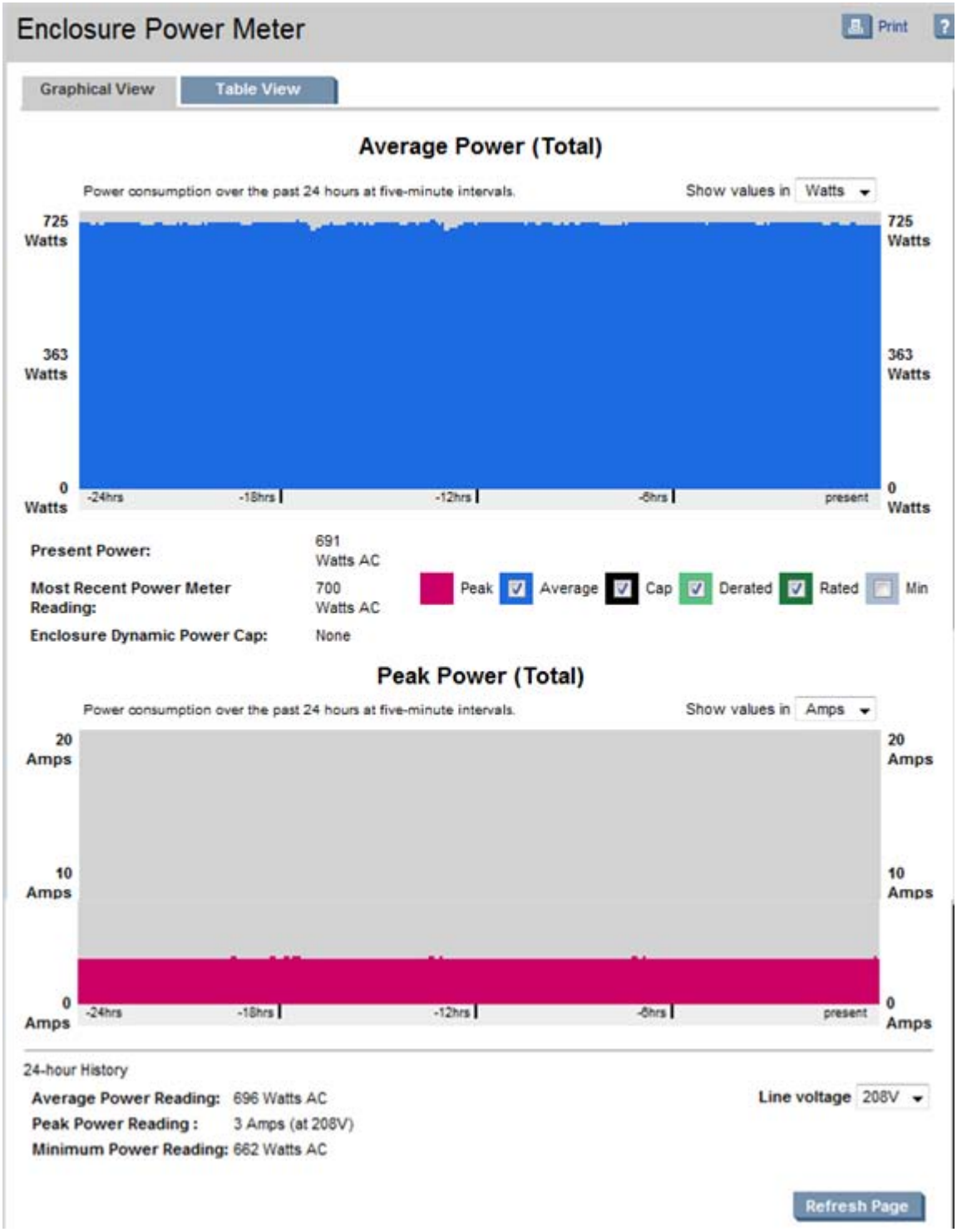
Les plafonds d'alimentation de serveur BladeSystem sont définis dans le module Onboard Administrator. Enclosure Dynamic Power Capping protège les infrastructures électriques et de refroidissement. Enclosure Dynamic Power Capping fonctionne avec la technologie de plafonnement de l'alimentation basée sur le microprogramme sur le serveur ou avec la technologie rapide, basée sur le matériel. La solution Enclosure Dynamic Power Capping fonctionne mieux si les lames de serveur qui prennent en charge la technologie rapide de plafonnement basée sur le matériel sont mises à jour.

Enclosure Dynamic Power Capping requiert Onboard Administrator 2.30 (ou ultérieure), iLO 2 version 1.70 (ou ultérieure) et une paire ROM/BIOS système datée du 01/10/2008 (ou ultérieure).

REMARQUE : Les plafonds d'alimentation définis pour moins de 50 % de la différence entre la puissance maximale et la puissance au ralenti peuvent devenir inaccessibles en raison de changements dans le serveur. Les plafonds d'alimentation définis pour moins de 20 % ne sont pas recommandés, et peuvent engendrer un redémarrage du serveur ou un arrêt de la réponse du système d'exploitation du serveur.

Écran Enclosure Power Meter

L'écran de jauge d'alimentation du boîtier affiche la consommation électrique de pointe, la consommation électrique moyenne, ainsi que l'alimentation allouée disponible sous forme d'un graphique qui permet d'interpréter facilement et rapidement la situation de l'alimentation du boîtier. La jauge d'alimentation est utile pour afficher les tendances en termes de consommation d'alimentation et peut aider à résoudre des problèmes du sous-système d'alimentation.



Onglet Graphical View

Cet écran permet de visualiser sous forme de graphique les lectures de consommation du boîtier.

Pour basculer entre watts, Btu/h et ampères, cliquez sur **Show Values** (Afficher les valeurs).

La valeur **Line Voltage** (Tension secteur) permet la conversion en ampères pour l'affichage. La valeur par défaut est basée sur le modèle du matériel de l'alimentation, et non sur la tension secteur réelle. Sélectionnez la tension secteur réelle pour le boîtier pour obtenir une conversion en ampères plus exacte.

Pour actualiser les informations de la jauge d'alimentation, cliquez sur **Refresh Page** (Actualiser la page).

Graphique des données de consommation moyenne

Ce graphique illustre la consommation électrique du boîtier au cours des 24 heures passées. Le module Onboard Administrator collecte les données de consommation électrique et de plafond d'alimentation dynamique du boîtier toutes les 5 minutes. Pour chaque période de cinq minutes, la consommation électrique maximale et moyenne ainsi que le plafond pour cette période sont stockés dans une mémoire tampon circulaire. Ces valeurs apparaissent sous la forme d'un graphique à barres, avec la valeur moyenne en bleu, la valeur maximale en rouge et la valeur de plafond en noir. Ces données sont réinitialisées au moment de la réinitialisation du boîtier. Vous pouvez choisir les informations fournies par le graphique à barres en activant ou en désactivant les cases à cocher **Average, Cap, Derated, Rated,** et **Min**.

Present Power (Puissance actuelle)

Cette valeur représente la puissance en watts consommée par tous les périphériques du boîtier.

Most Recent Power Meter Reading (Lecture de consommation la plus récente)

Cette valeur représente la lecture de consommation du boîtier la plus récente.

Graphique des données de consommation de pointe

Ce graphique montre la consommation électrique de pointe et Enclosure Dynamic Power Cap au cours des 24 heures passées.

Le libellé Peak Power (Consommation électrique de pointe) devient Peak Power (Side A + Side B) lorsque l'alimentation redondante N+N est active, indiquant une répartition du pic de consommation sur deux circuits. Deux graphiques apparaissent également : un pour Side A (Côté A) et un pour Side B (Côté B).

La répartition de la puissance entre le circuit A et le circuit B est estimée en fonction du nombre d'alimentations actives de chaque côté. En cas de perte de la redondance, le côté perdu affiche une consommation de pointe de zéro.

Enclosure Dynamic Power Cap (Limitation dynamique de la puissance du boîtier)

Cette valeur représente la lecture la plus récente du plafond d'alimentation dynamique du boîtier.

Average Power Reading (Lecture de consommation moyenne)

Cette valeur représente la moyenne des lectures de consommation du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur correspond à la moyenne de toutes les lectures depuis la mise sous tension du boîtier.

Peak Power Reading (Lecture de consommation de pointe)

Cette valeur représente les lectures de consommation de pointe du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur correspond au maximum de

toutes les lectures depuis la mise sous tension du boîtier ou la réinitialisation du module Onboard Administrator.

Le libellé Peak Power Reading (Lecture de consommation de pointe) devient Peak Power Reading (Side A + Side B) lorsque l'alimentation redondante N+N est active, indiquant une répartition du pic de consommation sur deux circuits.

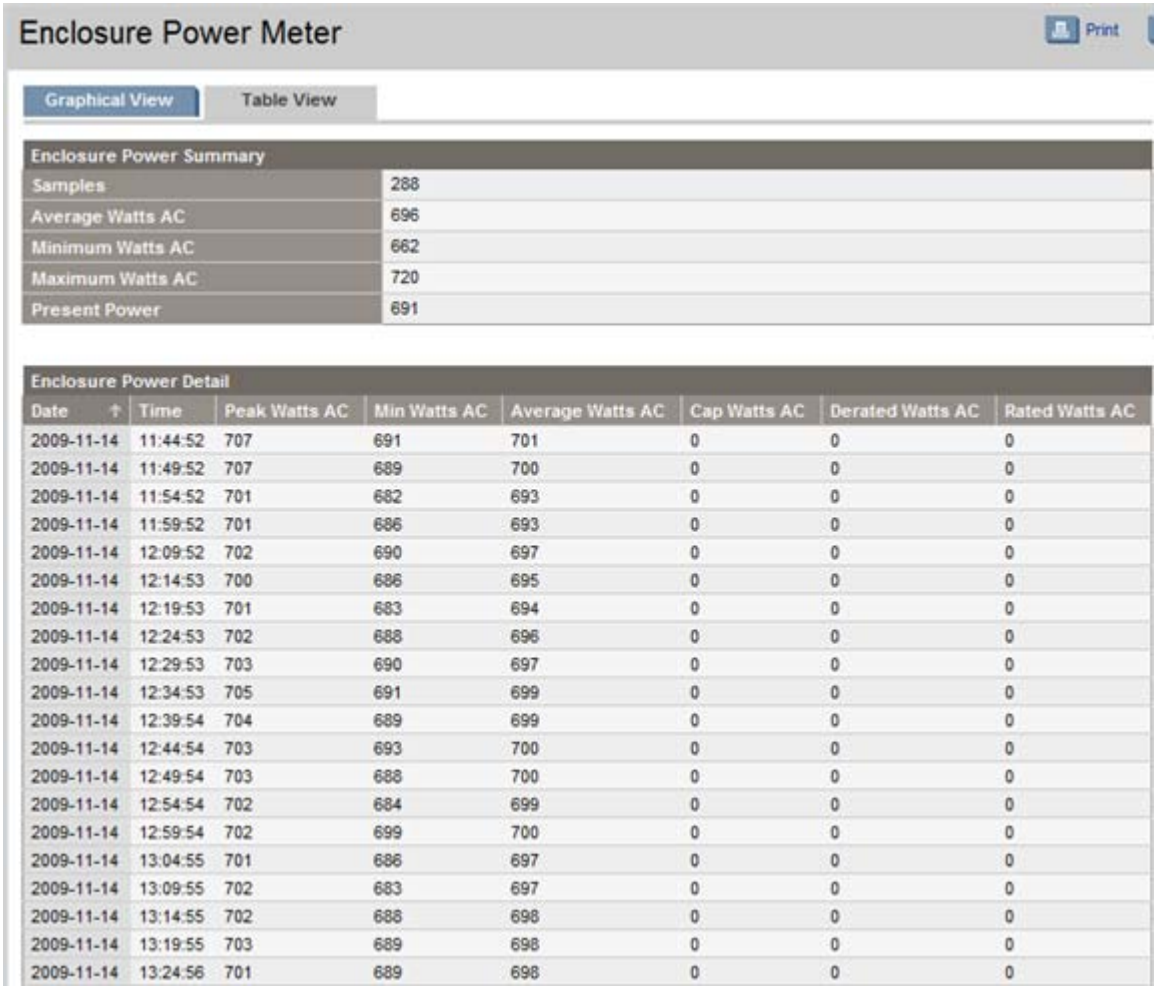
Minimum Power Reading (Lecture de consommation minimum)

Cette valeur représente les lectures de consommation minimum du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur correspond au minimum de toutes les lectures depuis la mise sous tension du boîtier.

Actualisation de la page

Lorsque vous redémarrez un boîtier, HP recommande d'attendre cinq minutes et d'appuyer ensuite sur le bouton **Refresh Page** (Actualiser la page) dans la mesure où la jauge d'alimentation n'est pas mise à jour de manière dynamique.

Onglet Table View



Cet écran permet de visualiser les lectures de consommation du boîtier sous forme de tableau.

Récapitulatif de la puissance du boîtier

Rangée	Description
Samples (Échantillons)	Nombre d'échantillons mesurés.
Average (Moyenne) (Watts, Btu/h ou Ampères)	Cette valeur correspond à la moyenne des lectures de consommation (Watts, Btu/h ou Ampères selon le critère sélectionné) du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur est la moyenne de toutes les lectures depuis la mise sous tension du boîtier.
Minimum (Watts, Btu/h ou Ampères)	Cette valeur représente les lectures de consommation minimum (Watts, Btu/h ou Ampères selon le critère sélectionné) du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur est le minimum de toutes les lectures depuis la mise sous tension du boîtier.
Maximum (Watts, Btu/h ou Ampères) (Side A + Side B)	Cette valeur représente les lectures de consommation maximum (Watts, Btu/h ou Ampères selon le critère sélectionné) du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur est le minimum de toutes les lectures depuis la mise sous tension du boîtier.
Present Power (Puissance actuelle)	Cette valeur affiche l'alimentation qui est consommée par tous les périphériques dans le boîtier.

Détails de consommation du boîtier

Le tableau de détails de consommation du boîtier fournit des informations détaillées pour chaque période d'échantillonnage de cinq minutes. Cliquez sur **Date** dans l'en-tête du tableau pour réorganiser l'ordre des informations détaillées de consommation du boîtier de la date actuelle à la date la plus ancienne ou inversement.

Colonne	Description
Date	La date de l'échantillon de lecture de consommation a été prise.
Time (Heure)	L'heure à laquelle l'échantillon de lecture de consommation a été prise.
Peak (Pointe (Watts, Btu/h ou Ampères)) (Side A + Side B)	Cette valeur représente les lectures de consommation maximum (Watts, Btu/h ou Ampères selon le critère sélectionné) du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur est le minimum de toutes les lectures depuis la mise sous tension du boîtier.
Min (Watts, Btu/h ou Ampères)	Cette valeur représente les lectures de consommation minimum (Watts, Btu/h ou Ampères selon le critère sélectionné) du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur est le minimum de toutes les lectures depuis la mise sous tension du boîtier.
Average (Moyenne) (Watts, Btu/h ou Ampères)	Cette valeur correspond à la moyenne des lectures de consommation (Watts, Btu/h ou Ampères selon le critère sélectionné) du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur est la moyenne de toutes les lectures depuis la mise sous tension du boîtier.

Colonne	Description
Cap (Plafond (Watts, Btu/h ou Ampères))	Cette valeur représente les lectures de plafond d'alimentation dynamique maximum (Watts, Btu/h ou Ampères selon le critère sélectionné) du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur est le minimum de toutes les lectures depuis la mise sous tension du boîtier.
Derated (Déclassé (Moyenne) (Watts, Btu/h ou Ampères))	Cette valeur représente les lectures de consommation déclassées (Watts, Btu/h ou Ampères selon le critère sélectionné) du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur est le minimum de toutes les lectures depuis la mise sous tension du boîtier.
Rated (Classé (Watts, Btu/h ou Ampères))	Cette valeur représente les lectures de consommation classées (Watts, Btu/h ou Ampères selon le critère sélectionné) du boîtier sur la dernière période de 24 heures. Si le boîtier n'a pas été alimenté pendant 24 heures, la valeur est le minimum de toutes les lectures depuis la mise sous tension du boîtier.

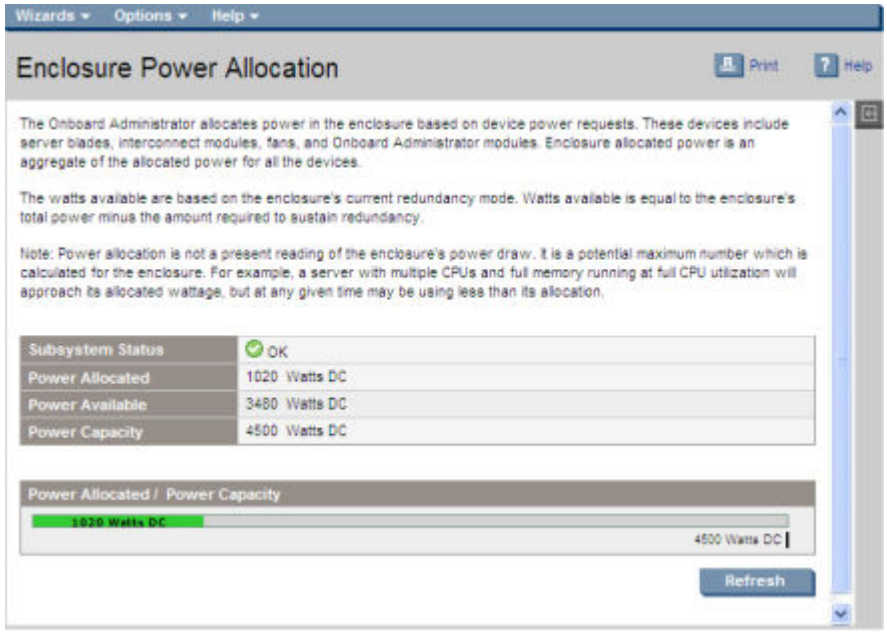
Power units (Unités d'alimentation)

Sélectionnez la valeur dans laquelle afficher la date d'alimentation à partir du menu.

Line voltage (Tension secteur)

Sélectionnez la tension secteur appropriée dans le menu.

Allocation de l'alimentation du boîtier


Wizards
Options
Help
Enclosure Power Allocation
Print
Help
The Onboard Administrator allocates power in the enclosure based on device power requests. These devices include server blades, interconnect modules, fans, and Onboard Administrator modules. Enclosure allocated power is an aggregate of the allocated power for all the devices.
The watts available are based on the enclosure's current redundancy mode. Watts available is equal to the enclosure's total power minus the amount required to sustain redundancy.
Note: Power allocation is not a present reading of the enclosure's power draw. It is a potential maximum number which is calculated for the enclosure. For example, a server with multiple CPUs and full memory running at full CPU utilization will approach its allocated wattage, but at any given time may be using less than its allocation.
Subsystem Status
OK
Power Allocated
1020 Watts DC
Power Available
3480 Watts DC
Power Capacity
4500 Watts DC
Power Allocated / Power Capacity
1020 Watts DC
4500 Watts DC
Refresh

L'écran Power Allocation (Allocation de l'alimentation) affiche des informations de base concernant la capacité totale, la capacité redondante et l'alimentation allouée en watts du sous-système d'alimentation. Le graphique Enclosure Internal Power (Alimentation interne du boîtier) affiche le nombre de watts attribués en vert sur un fond gris, qui représente la capacité redondante totale des alimentations.

Si vous modifiez le mode de redondance du boîtier après l'allocation de l'alimentation aux périphériques, le sous-système d'alimentation peut devenir dégradé. L'alimentation est toujours allouée aux périphériques, mais la redondance peut ne pas fonctionner correctement. Si des puissances nulles sont disponibles et que le graphique d'alimentation affiche une condition dégradée, vérifiez votre sous-système d'alimentation et les configurations de redondance. Vous pouvez résoudre la condition dégradée en modifiant votre mode de redondance ou en ajoutant d'autres blocs d'alimentation au boîtier.

La capacité d'alimentation sera égale à l'alimentation allouée en cas de perte de la redondance.

Récapitulatif de la puissance du boîtier

Récapitulatif de la puissance d'entrée du boîtier :

La puissance actuelle est l'entrée en watts appliquée au boîtier, mesurée en watts CA pour les blocs d'alimentation dotés d'entrées CA et mesurée en watts CC pour les blocs d'alimentation dotés d'entrées CC. La puissance d'entrée max est l'entrée la plus élevée prévue en watts. Si une limite d'alimentation est définie, la puissance d'entrée max est égale à la limite d'alimentation. Si un plafond d'alimentation dynamique de boîtier est défini et que EDPC est activé, la puissance d'entrée max est égale au plafond d'alimentation dynamique de boîtier. Si ni la limite d'alimentation ni le plafond d'alimentation dynamique de boîtier n'est défini, la puissance d'entrée max du boîtier est la puissance d'entrée prévue pour que le boîtier fonctionne suivant la capacité maximum de sortie CC.

Récapitulatif de la puissance de sortie du boîtier :

Lorsque EDPC est désactivé, la capacité d'alimentation est basée sur le nombre de blocs d'alimentation installés et fonctionnels, leurs capacités de sortie CC et le paramètre de mode d'alimentation redondant. La puissance allouée est la puissance de sortie totale du boîtier allouée aux baies de périphérique, baies d'interconnexion et ventilateurs. La puissance disponible est la capacité d'alimentation moins la puissance allouée.

Lorsque EDPC est activé, la capacité d'alimentation est le plafond d'alimentation dynamique du boîtier en watts CC. La puissance allouée est l'alimentation minimum à laquelle le boîtier peut être plafonné en watts CC. La puissance disponible est la capacité d'alimentation moins la puissance allouée. La puissance totale allouée aux baies de périphérique, baies d'interconnexion et ventilateurs peut ne pas être égale à la puissance allouée pour les boîtiers dans la mesure où le plafond d'alimentation sur chaque serveur est contrôlé dynamiquement.

Allocation de puissance de sortie de baies de périphériques :

La puissance allouée dans le boîtier est le total des allocations de puissance pour l'ensemble des baies de périphérique, baies d'interconnexion et ventilateurs.

Récapitulatif de puissance de baies de périphériques :

Chaque baie de périphérique remplie est répertoriée avec la puissance allouée. Si EDPC est activé, des colonnes supplémentaires indiquent les valeurs Plafond d'alimentation, Plafond d'alimentation % et Puissance actuelle compatibles du serveur ProLiant. La valeur Plafond d'alimentation % est calculée sur la base du plafond d'alimentation en watts actuel divisé par la puissance en watts allouée. Si EDPC est activé, une lame de serveur demandant une alimentation est uniquement autorisée à s'allumer si la puissance disponible prend en charge la demande ou que le module Onboard Administrator peut modifier le plafond d'alimentation d'autres serveurs afin de prendre en charge la demande.

Récapitulatif de puissance de baies d'interconnexion :

Chaque baie d'interconnexion remplie est répertoriée avec la puissance allouée.

Récapitulatif de puissance de ventilateurs :

La puissance des ventilateurs est allouée sur la base de la règle des ventilateurs. La règle des ventilateurs est déterminée en fonction du type de boîtier (c3000 ou c7000) et des baies de périphériques occupées. L'allocation de puissance pour les ventilateurs et la consommation totale de puissance actuelle de tous les ventilateurs sont répertoriées.

Pour mettre à jour les informations de récapitulatif de puissance, cliquez sur le bouton **Refresh** (Actualiser).

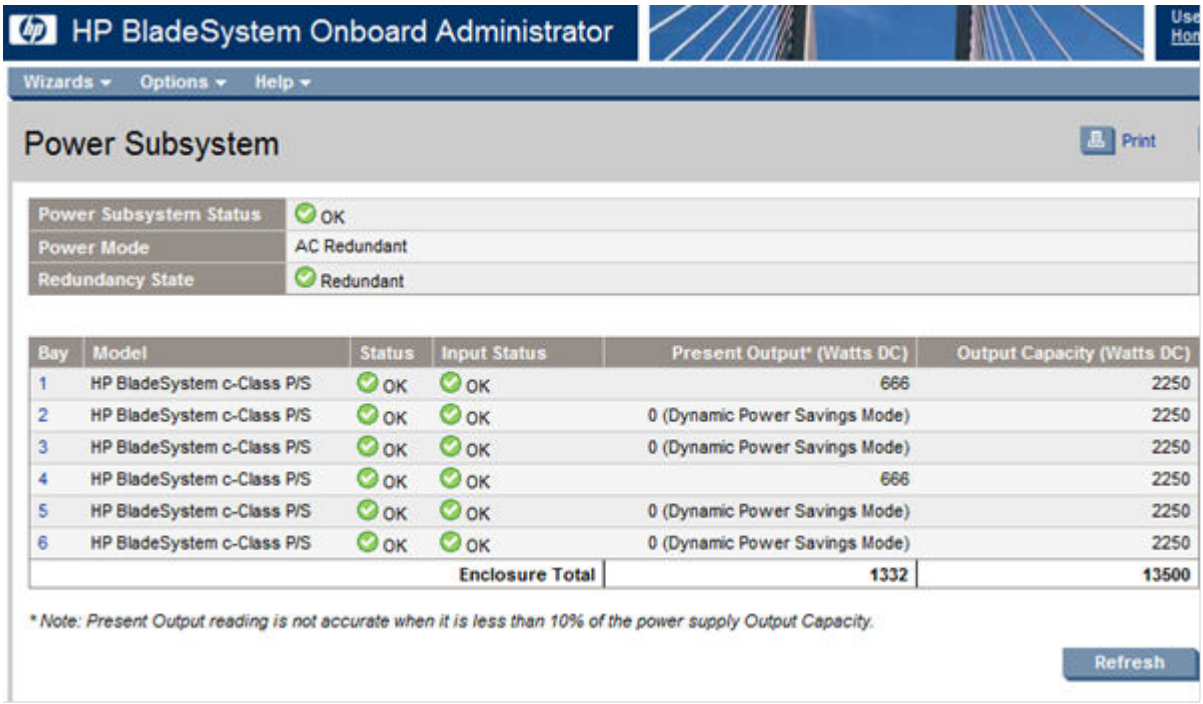
Écran Power Subsystem

Alimentations disponibles dans les boîtiers BladeSystem

Toutes les alimentations dans un boîtier doivent porter la même référence. Le module Onboard Administrator vous signale quelles alimentations doivent être remplacées en affichant une icône d'avertissement.

Power Supply summary (Résumé de l'alimentation)

L'écran Power Subsystem (Sous-système d'alimentation) fournit l'état du sous-système d'alimentation, sur chaque alimentation individuelle, ainsi que les conditions de panne.


HP BladeSystem Onboard Administrator
Wizards
Options
Help
Power Subsystem
Print
Power Subsystem Status
OK
Power Mode
AC Redundant
Redundancy State
Redundant
Bay
Model
Status
Input Status
Present Output* (Watts DC)
Output Capacity (Watts DC)
1 HP BladeSystem c-Class P/S OK OK 666 2250
2 HP BladeSystem c-Class P/S OK OK 0 (Dynamic Power Savings Mode) 2250
3 HP BladeSystem c-Class P/S OK OK 0 (Dynamic Power Savings Mode) 2250
4 HP BladeSystem c-Class P/S OK OK 666 2250
5 HP BladeSystem c-Class P/S OK OK 0 (Dynamic Power Savings Mode) 2250
6 HP BladeSystem c-Class P/S OK OK 0 (Dynamic Power Savings Mode) 2250
Enclosure Total 1332 13500
* Note: Present Output reading is not accurate when it is less than 10% of the power supply Output Capacity.
Refresh

Cet écran présente l'état du sous-système d'alimentation et de chaque alimentation individuelle.

Sous-système d'alimentation

Rangée	Description
Power Subsystem Status (État de l'alimentation du sous-système)	État du sous-système d'alimentation. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Critical Error (Erreur critique).
Power Mode (Mode d'alimentation)	Paramètre utilisateur destiné à configurer la capacité de puissance CC du boîtier et le mode de redondance d'entrée du boîtier. Les valeurs possibles sont Redundant (Redondant), AC Redundant (Redondance secteur), Power

Rangée	Description
	Supply Redundant (Alimentation redondante), Not Redundant (Non redondant) et Unknown (Inconnu).
Redundancy State (État de redondance)	Indique l'état de redondance du sous-système d'alimentation. Les valeurs possibles sont Redundant (Redondant), Not Redundant (Non redondant) ou Redundancy (Redondance perdue).

État de l'alimentation

Colonne	Description
Bay (Baie)	Baie dans le boîtier de l'alimentation correspondante. Ce champ affiche uniquement les baies peuplées. Les baies vides n'apparaissent pas dans ce tableau.
Model (Modèle)	Nom de modèle de l'alimentation.
Status (État)	État global de l'alimentation. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Critical Error (Erreur critique).
Input Status (État de l'entrée)	État de l'entrée de l'alimentation. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Critical Error (Erreur critique).
Present Output (Watts) (Sortie présente)	Cette valeur est une mesure de la sortie présente de l'alimentation en watts.
Output Capacity (Watts) (Capacité de sortie)	Quantité de puissance fournie par l'alimentation, affichée en watts. Mesure de la sortie en watts CC générée par l'alimentation.

Cliquez sur **Refresh** (Actualiser) pour actualiser les informations du sous-système d'alimentation.

Informations d'alimentation

La sélection d'une alimentation spécifique ouvre la page Power Supply Information—Bay x (Informations sur l'alimentation—Baie x), où x est la baie de l'alimentation sélectionnée. Cet écran fournit des informations sur l'état de l'alimentation sélectionnée.

Informations d'état

Rangée	Description
Status (État)	État global de l'alimentation. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Critical Error (Erreur critique).
Input Status (État de l'entrée)	État de l'entrée de l'alimentation. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Critical Error (Erreur critique).
Present Output (Sortie présente)	Quantité de puissance fournie par l'alimentation en mode CA ou CC. Cette valeur est affichée en watts.
Output Capacity (Capacité de sortie)	Quantité de puissance qui peut être fournie par l'alimentation en mode CA ou CC. Cette valeur est affichée en watts.

Rangée	Description
Model (Modèle)	Nom de modèle de l'alimentation.
Serial Number (Numéro de série)	Numéro de série unique de l'alimentation.
Part Number (Référence)	Numéro de référence à utiliser pour commander une alimentation de ce type supplémentaire ou de remplacement.
Spare Part Number (Numéro de la pièce de rechange)	Numéro de pièce de rechange à utiliser pour commander une alimentation supplémentaire ou de remplacement.

Informations de diagnostics

Les informations de diagnostics sont recueillies de deux façons : Par interrogation du microcontrôleur de périphérique (résultat d'un état détérioré si une panne s'est produite) ou envoyées par le microcontrôleur du périphérique, sans interrogation, pour signaler une panne.

Rangée	Description
Device Identification Data (Données d'identification du périphérique)	Les données d'identification de périphérique contrôlées sont des informations telles que le nom du modèle, la référence, le numéro de série, ainsi que d'autres informations utilisées pour identifier le périphérique. Ces données sont également appelées données FRU. Une erreur de données d'identification du périphérique s'affiche si les données sont absentes ou illisibles par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Device Location (Emplacement du périphérique)	Emplacement d'alimentation incorrect. Les valeurs possibles sont OK et Incorrect location for proper device cooling (Emplacement incorrect pour refroidissement correct du périphérique).
Device Operational (Périphérique fonctionnel)	Échec du périphérique. L'état n'a pas été demandé par le Onboard Administrator. Les valeurs possibles sont OK et Error.
Device Degraded (Périphérique détérioré)	Échec du périphérique. L'état a été demandé par le Onboard Administrator. Les valeurs possibles sont OK et Error.
Power Cord (Cordon d'alimentation)	État de la tension d'entrée. Les valeurs possibles sont OK et Error.
Device Mismatch (Discordance de périphériques)	Ce champ indique si différents modèles d'alimentation sont installés dans le même boîtier et si vous devez installer les mêmes modèles d'alimentation dans chaque baie.
Service Action (Action de service)	Action de service recommandée requise pour corriger une erreur d'alimentation.

Cliquez sur **Refresh** (Actualiser) pour actualiser les informations du module d'alimentation.

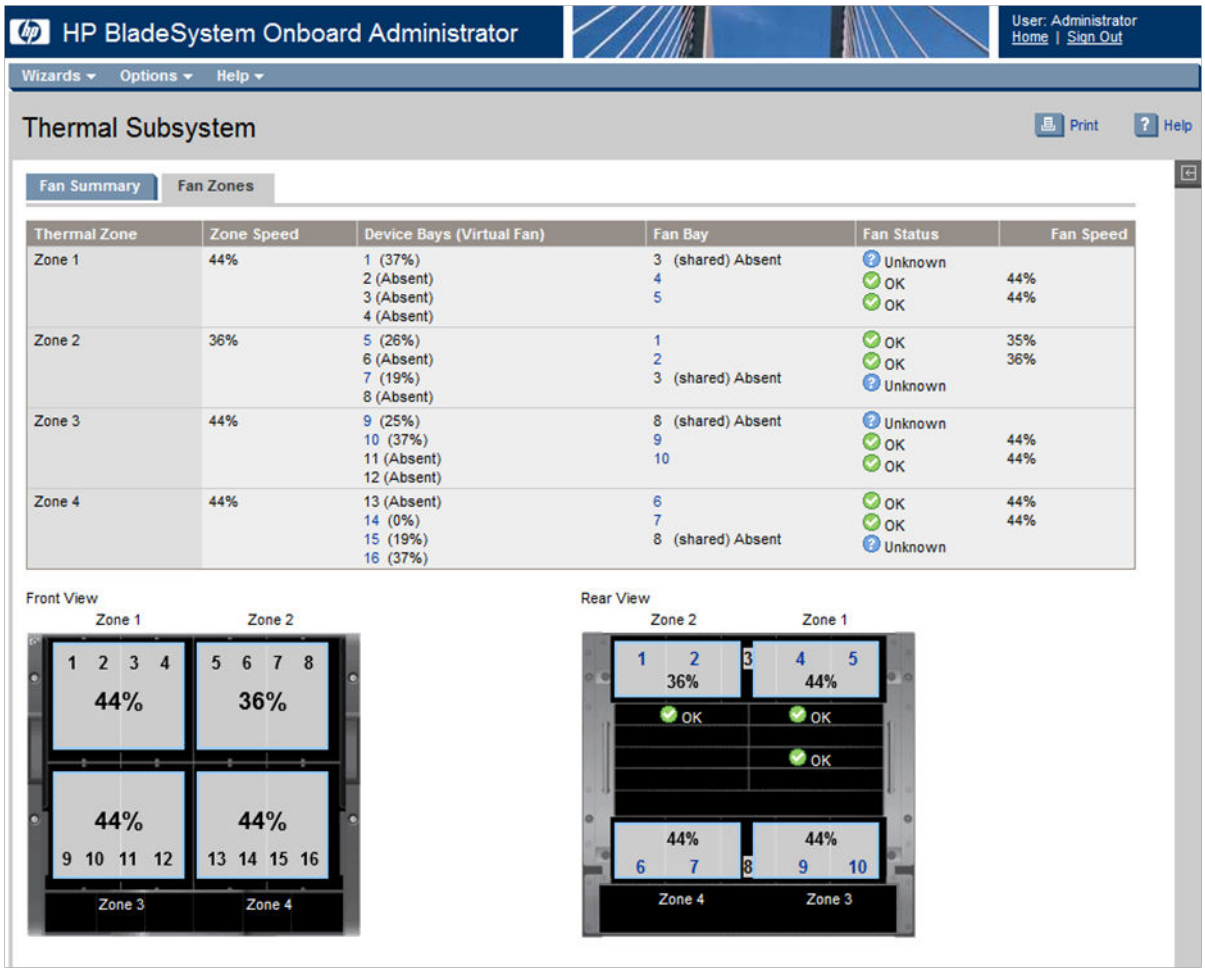
Gestion des ventilateurs et de la ventilation

Zones de ventilateur

Les zones de ventilateur permettent de contrôler l'état et l'efficacité de la ventilation des baies pour lesquelles des ventilateurs ont été affectés. Les vitesses consignées pour ces zones correspondent à

des vitesses cibles. Ces valeurs évoluent au fil du temps, en fonction des changements de vitesse des ventilateurs pour répondre aux besoins de ventilation de la zone. L'écran Fan Zones (Zones de ventilateur) n'est pas actualisé dynamiquement. Pour mettre à jour les informations sur cet écran, cliquez sur le bouton **Refresh** (Actualiser).

Les vitesses de ventilateur sont indiquées en pourcentage de la capacité totale, et les ventilateurs fonctionnant dans une zone sans lame tournent à une vitesse RPM minimum de 30 % pour conserver un refroidissement correct de tout le boîtier.


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
Wizards
Options
Help
Thermal Subsystem
Print
Help
Fan Summary
Fan Zones
Thermal Zone | Zone Speed | Device Bays (Virtual Fan) | Fan Bay | Fan Status | Fan Speed
Zone 1 | 44% | 1 (37%) 2 (Absent) 3 (Absent) 4 (Absent) | 3 (shared) Absent 4 5 | Unknown OK OK | 44% 44%
Zone 2 | 36% | 5 (26%) 6 (Absent) 7 (19%) 8 (Absent) | 1 2 3 (shared) Absent | OK OK Unknown | 35% 36%
Zone 3 | 44% | 9 (25%) 10 (37%) 11 (Absent) 12 (Absent) | 8 (shared) Absent 9 10 | Unknown OK OK | 44% 44%
Zone 4 | 44% | 13 (Absent) 14 (0%) 15 (19%) 16 (37%) | 6 7 8 (shared) Absent | OK OK Unknown | 44% 44%
Front View
Zone 1
Zone 2
1 2 3 4
44%
5 6 7 8
36%
44%
9 10 11 12
44%
13 14 15 16
Zone 3
Zone 4
Rear View
Zone 2
Zone 1
1 2
36%
3
4 5
44%
OK
OK
OK
44%
6 7
8
44%
9 10
Zone 4
Zone 3

Colonne	Description
Thermal Zone (Zone thermique)	Les quatre zones de refroidissement dans le boîtier : en haut à gauche, en haut à droite, en bas à gauche et en bas à droite
Zone Speed (Vitesse dans la zone)	Vitesse de ventilateur requise calculée en fonction du périphérique devant être le plus ventilé dans la zone.
Device Bays (Baies de périphérique)	Numéro des baies de périphériques dans une zone thermique donnée.
Fan Bay (Baie de ventilateur)	Numéro de baie de ventilateur. Les ventilateurs dans les baies 3 et 8 se partagent les zones thermiques.

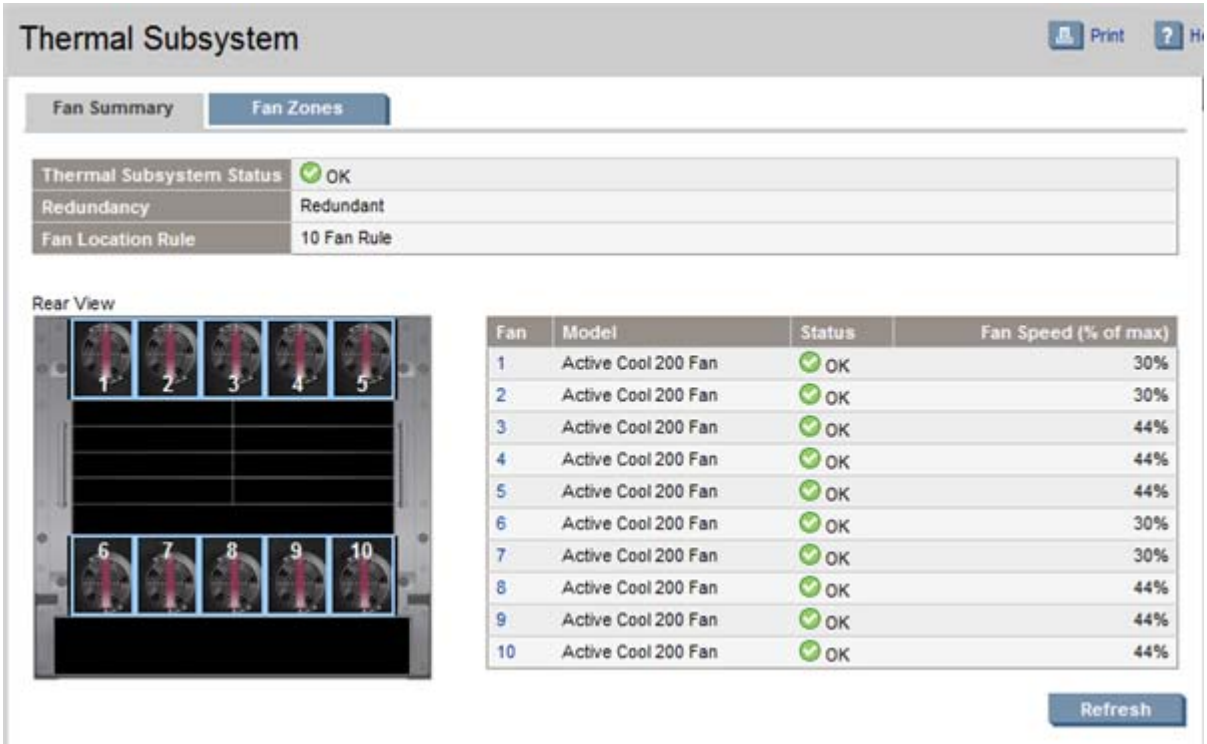
Colonne	Description
Fan Status (État du ventilateur)	État global de chaque ventilateur. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré), Failed (Échec) et Absent.
Fan Speed (Vitesse du ventilateur)	Pourcentage du nombre de tours par minute maximum.

Sous-système thermique

Le module Onboard Administrator surveille jusqu'à 10 ventilateurs dans le boîtier et ajuste les vitesses de ventilateur suivant les besoins, sur la base des mesures thermiques et d'alimentation. La vitesse de chaque ventilateur peut être réglée pour réduire le niveau de bruit et la consommation d'énergie, de même que pour compenser les différences de débit d'air à l'intérieur du boîtier. Les performances de chaque ventilateur sont contrôlées et le module Onboard Administrator consigne chaque erreur ou avertissement dans le journal système et HP SIM (si SNMP est activé).

La surveillance des zones de ventilateur est uniquement disponible sur le boîtier c7000. Toutes les autres fonctions et fonctionnalités du sous-système thermique sont les mêmes pour les boîtiers c3000 et c7000, sauf dans le cas des exceptions mentionnées.

L'écran suivant illustre la page Fan Summary (Résumé des ventilateurs) pour un boîtier c7000.



Fan Summary (Résumé des ventilateurs)

Cet écran présente l'état du sous-système thermique et de chaque ventilateur individuel.

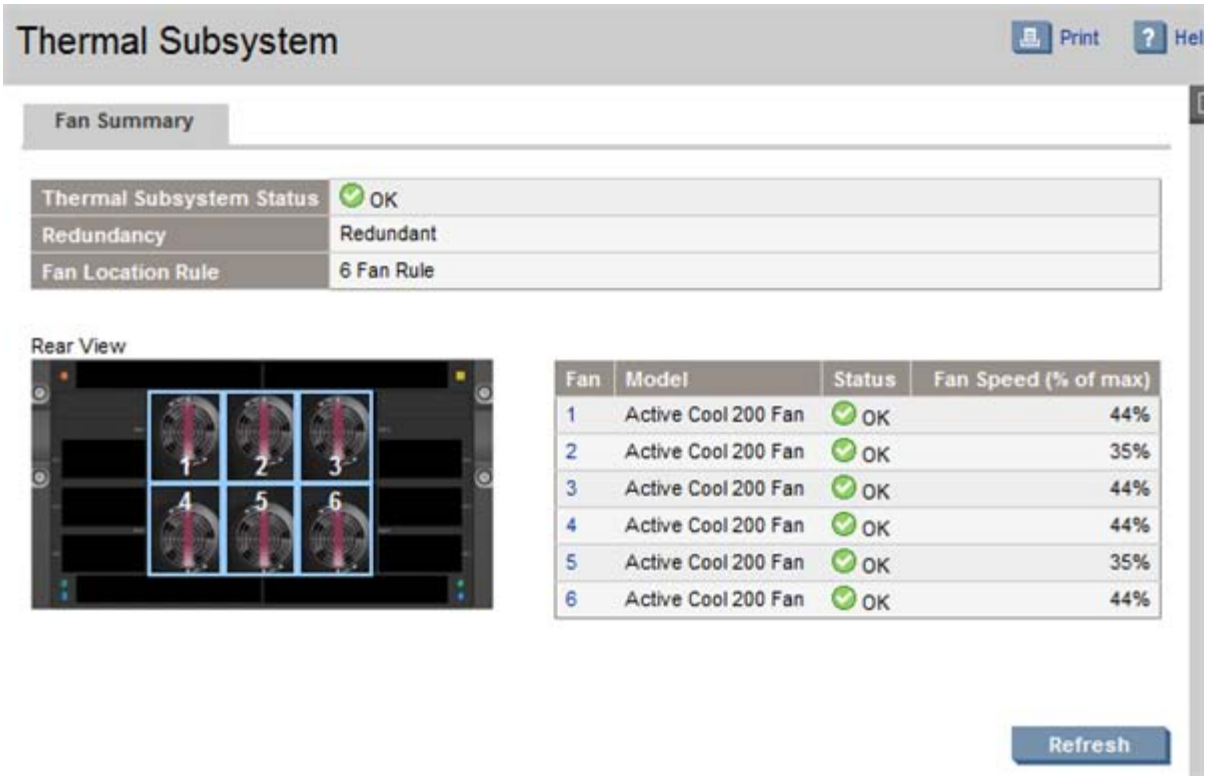
État du sous-système de ventilateurs

Rangée	Description
Thermal Subsystem Status (État thermique du sous-système)	Indique l'état global du sous-système de ventilateurs. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré) et Critical Error (Erreur critique).
Redundancy (Redondance)	Indique l'état de redondance des ventilateurs. Les valeurs possibles sont Redundant (Redondant) et Not Redundant (Non redondant).
Fan Location Rule (Règle d'emplacement des ventilateurs)	La règle d'emplacement des ventilateurs indique l'emplacement correct des ventilateurs et les baies de périphériques prises en charge.

État du ventilateur

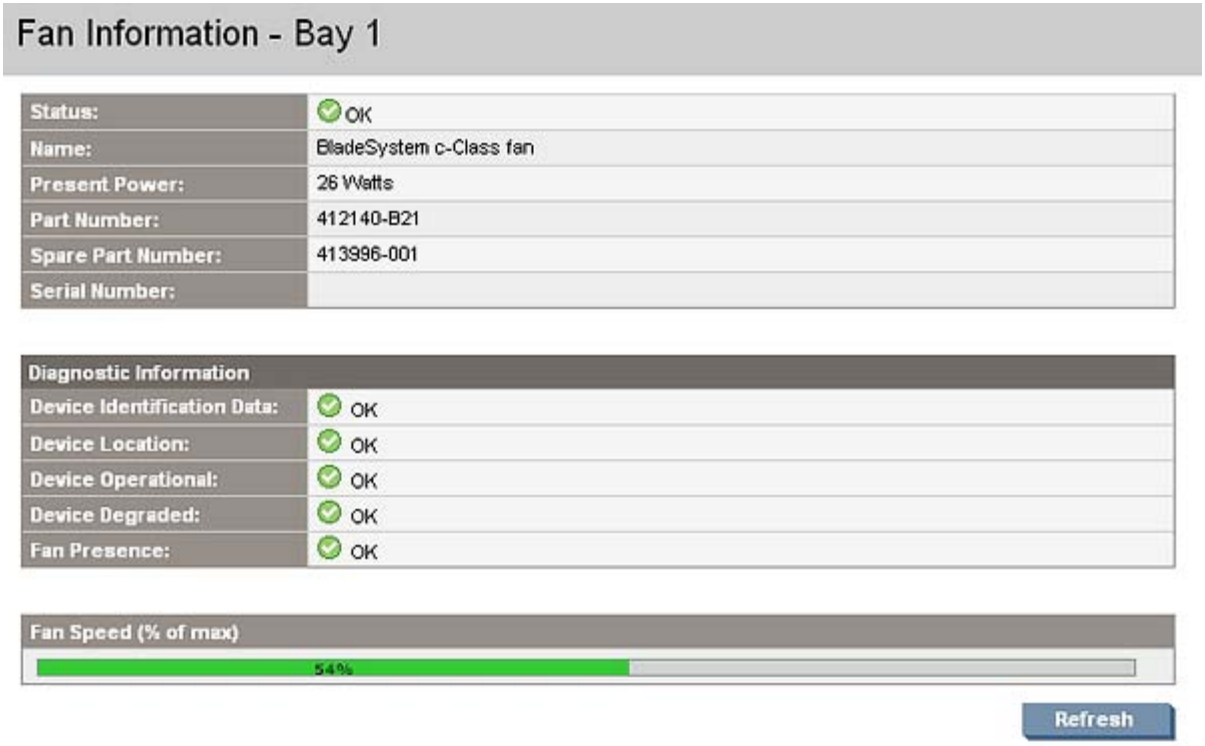
Colonne	Description
Fan (Ventilateur)	Baie dans le boîtier du ventilateur correspondant.
Model (Modèle)	Nom du modèle de ventilateur.
Status (État)	Indique l'état global du ventilateur. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré), Failed (Échec) et Absent.
Fan Speed (Vitesse du ventilateur)	Indique la vitesse du ventilateur sous forme de pourcentage du nombre de tours par minute maximum.

L'écran suivant illustre la page Fan Summary (Résumé des ventilateurs) pour un boîtier c3000.

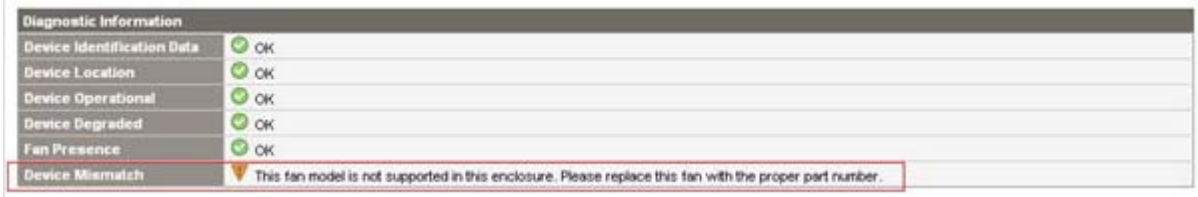


En cas de panne d'un module de ventilateur, les ventilateurs restants compensent automatiquement en ajustant les vitesses de ventilateur.

Vous pouvez afficher l'état de chaque ventilateur en le sélectionnant dans la navigation d'arborescence ou la navigation graphique. L'écran Fan Information (Informations sur le ventilateur) fournit des informations sur l'état global du ventilateur, son nom, la puissance consommée en watts, son numéro de référence, le numéro de pièce de rechange et son numéro de série. L'écran d'informations de ventilateurs inclut également des informations de diagnostic, telles que les erreurs de données internes, les erreurs d'emplacement, les défauts de périphérique, la dégradation de périphérique et la discordance de périphériques. Les vitesses de ventilateur sont indiquées en tours par minute (RPM). Pour mettre à jour les informations sur cette page, cliquez sur le bouton **Refresh** (Actualiser).



Cet écran affiche une erreur de discordance de ventilateurs.


Diagnostic Information
Device Identification Data OK
Device Location OK
Device Operational OK
Device Degraded OK
Fan Presence OK
Device Mismatch This fan model is not supported in this enclosure. Please replace this fan with the proper part number.

La sélection d'un ventilateur spécifique ouvre la page Fan Information, Bay *x* (Informations sur le ventilateur - Baie x), où *x* est la baie du ventilateur sélectionné. Cet écran fournit des informations d'état sur le ventilateur sélectionné.

Informations d'état

Rangée	Description
Status (État)	État global du ventilateur. Les valeurs possibles sont Unknown (Inconnu), OK, Degraded (Détérioré), Failed (Échec) et Other (Autre).

Rangée	Description
Name (Nom)	Nom descriptif commun du ventilateur.
Present Power (Puissance actuelle)	Quantité d'alimentation consommée par le ventilateur.
Part Number (Référence)	Numéro de référence à utiliser pour commander un ventilateur de ce type supplémentaire ou de remplacement.
Spare Part Number (Numéro de la pièce de rechange)	Numéro de pièce de rechange à utiliser pour commander un ventilateur supplémentaire ou de remplacement.
Serial Number (Numéro de série)	Numéro de série unique du ventilateur.

Informations de diagnostics

Les informations de diagnostics sont recueillies de deux façons : Par interrogation du microcontrôleur de périphérique (résultat d'un état détérioré si une panne s'est produite) ou envoyées par le microcontrôleur du périphérique, sans interrogation, pour signaler une panne.

Rangée	Description
Device Identification Data (Données d'identification du périphérique)	Contient des informations telles que le nom du modèle, la référence, le numéro de série, ainsi que d'autres informations utilisées pour identifier le périphérique. Ces données sont également appelées données FRU. Une erreur de données d'identification du périphérique s'affiche si les données sont absentes ou illisibles par le module Onboard Administrator. Les valeurs possibles sont OK et Error.
Device Location (Emplacement du périphérique)	Incorrect fan location (Emplacement incorrect du ventilateur). Les valeurs possibles sont OK et Incorrect location for proper device cooling (Emplacement incorrect pour refroidissement correct du périphérique).
Device Operational (Périphérique fonctionnel)	Échec du périphérique. L'état n'a pas été demandé par le Onboard Administrator.
Device Degraded (Périphérique détérioré)	Échec du périphérique. L'état a été demandé par le Onboard Administrator.
Fan Presence (Présence du ventilateur)	Ce champ indique si un ventilateur est requis pour prendre en charge la règle des ventilateurs actuelle.
Device Mismatch (Discordance de périphériques)	Ce champ indique si différents modèles de ventilateur sont installés dans le même boîtier et si vous devez installer les mêmes modèles de ventilateur dans chaque baie.

Modèles de ventilateur

Le boîtier c3000 prend en charge les modèles de ventilateur Active Cool 100 et Active Cool 200. Le boîtier c7000 prend uniquement en charge les modèles de ventilateur Active Cool 200. Vous ne pouvez pas mélanger des modèles de ventilateur dans le boîtier c3000. Si vous mélangez des modèles de ventilateur ou que vous placez le modèle de ventilateur incorrect dans le boîtier, une erreur **Device Mismatch** (Discordance de ventilateurs) apparaît dans le tableau Diagnostic Information (Informations de diagnostics).

Pour mettre à jour les informations de ventilateurs, cliquez sur le bouton **Refresh** (Actualiser).

Pour installer correctement les ventilateurs dans le boîtier, consultez le Manuel d'installation et de configuration du boîtier HP BladeSystem c7000.

Règles d'emplacement des ventilateurs du boîtier c7000

Le boîtier HP BladeSystem c7000 est livré avec au moins quatre ventilateurs HP Active Cool 200 et prend en charge jusqu'à 10 ventilateurs. Vous devez installer les ventilateurs par groupes pairs, sur la base du nombre total de lames de serveur installées dans le boîtier. Installez des caches de ventilateur dans les baies de ventilateur non utilisées.

Règle pour quatre ventilateurs

Les baies de ventilateur 4, 5, 9 et 10 sont utilisées pour toute combinaison prise en charge de lames de serveur occupant un maximum de deux baies de périphérique situées dans les baies de périphérique 1, 2, 9 ou 10.

Règle pour six ventilateurs

Les baies de ventilateur 3, 4, 5, 8, 9 et 10 sont utilisées pour toute combinaison prise en charge de lames de serveur occupant un maximum de huit baies de périphérique situées dans les baies de périphérique 1, 2, 3, 4, 9, 10, 11 ou 12.

Règle pour huit ventilateurs

Les baies de ventilateur 1, 2, 4, 5, 6, 7, 9 et 10 sont utilisées pour toute combinaison prise en charge de lames de serveur dans toutes les baies de périphérique.

Règle pour dix ventilateurs

Toutes les baies de ventilateur sont utilisées pour toute combinaison prise en charge de lames de serveur dans toutes les baies de périphérique.

Règles générales de ventilateurs

- 6 ventilateurs au minimum sont nécessaires pour tout boîtier configuré avec un module d'entrée d'alimentation triphasée.
- 8 ventilateurs au minimum sont nécessaires si au moins un module de commutation est installé dans la baie d'interconnexion 1, 3, 5 ou 7 et au moins un module de commutation est installé dans la baie d'interconnexion 2, 4, 6 ou 8. Cela ne s'applique pas aux modules pass-thru.
- Dix ventilateurs sont requis pour une configuration avec :
  - Un ou plusieurs modules HP Virtual Connect FlexFabric-20/40 F8
  - Une ou plusieurs lames de stockage D2220sb
  - Plus de la moitié des baies de périphérique de boîtier occupées et n'importe quel nombre de lames de stockage D2200sb présentes
  - Au minimum neuf lames de serveur HP BL460c G1 et/ou HP BL460c G5

  REMARQUE : Pour fournir une redondance et une efficacité de refroidissement maximum, une consommation d'énergie réduite et un niveau de bruit réduit, HP recommande vivement dix ventilateurs pour toutes les configurations.

Règles d'emplacement des ventilateurs du boîtier c3000

Le boîtier HP BladeSystem c3000 est livré avec quatre ventilateurs HP Active Cool 100 et prend en charge jusqu'à six ventilateurs. Vous devez installer les ventilateurs par groupes pairs, sur la base du nombre total de lames de serveur installées dans le boîtier. Installez des caches de ventilateur dans les baies de ventilateur non utilisées.

Règle pour quatre ventilateurs

Pour une à quatre lames de serveur ou de stockage demi-hauteur, ou une à deux lames de serveur ou de stockage pleine hauteur, utilisez les baies de ventilateur 2, 4, 5 et 6 pour prendre en charge un maximum de quatre baies de périphérique situées dans les baies de périphérique 1, 2, 5 ou 6.

Règle pour six ventilateurs

Pour des lames de serveur ou de stockage supplémentaires, installez six ventilateurs en utilisant toutes les baies de périphérique.

REMARQUE : Vous ne pouvez pas installer des ventilateurs HP Active Cool 100 et des ventilateurs HP Active Cool 200 dans le même boîtier. Le module Onboard Administrator envoie un message d'erreur, et vous devez retirer le type de ventilateur ayant le nombre inférieur d'unités installées.

Gestion des utilisateurs

Authentification des utilisateurs

Cette section décrit les niveaux de droits utilisateur reconnus par le module HP BladeSystem Onboard Administrator et présente des procédures détaillées pour configurer les fonctionnalités de gestion fournies par le module Onboard Administrator.

L'option de menu Users/Authentication (Utilisateurs/Authentification) ne peut pas être sélectionnée et n'affiche pas d'informations d'ensemble pour les comptes ou les paramètres utilisateur. Sélectionnez plutôt l'une des options du sous-menu pour les paramètres spécifiques.

Rôles et niveaux de privilège utilisateur

Dans la catégorie Users/Authentication (Utilisateurs/Authentification) du HP BladeSystem Onboard Administrator, vous pouvez accéder à la sous-catégorie Local Users (Utilisateurs locaux). Dans cette sous-catégorie, vous pouvez créer des comptes utilisateur, employés par des utilisateurs individuels pour se connecter au module HP Onboard Administrator, et qui possèdent un nom utilisateur, un mot de passe et, généralement, des informations de contact. L'un des trois niveaux de privilège suivants peut être attribué aux utilisateurs :

- **ADMINISTRATOR** (Administrateur) permet d'accéder à tous les aspects du module HP BladeSystem Onboard Administrator, y compris la configuration, les mises à jour de microprogramme, la gestion des utilisateurs et la réinitialisation sur les paramètres par défaut.
- **OPERATOR** (Opérateur) permet d'accéder à toutes les informations, mais seuls certains paramètres de configuration peuvent être modifiés. Ce compte est utilisé pour les individus qui peuvent avoir à modifier périodiquement des paramètres de configuration.
- **USER** (Utilisateur) permet d'accéder à toutes les informations, mais sans possibilité de modifier les paramètres HP BladeSystem Onboard Administrator. Ce compte est utilisé pour les personnes ayant besoin de visualiser la configuration du module HP BladeSystem Onboard Administrator, mais pour lesquelles la capacité de modifier des paramètres n'est pas nécessairement utile.

Basée sur des autorisations utilisateur, l'approche des niveaux de privilège du HP BladeSystem Onboard Administrator facilite la maintenance des baies de lame de serveur. Cette approche fonctionne selon les principes suivants :

- Des niveaux de privilège sont attribués aux utilisateurs dans User Management (Gestion des utilisateurs).
- Un utilisateur peut accéder à la combinaison de baies de périphérique, de baies d'interconnexion et de baies de module Onboard Administrator de son choix.

L'accès à une lame de serveur par un utilisateur dépend du niveau de privilège attribué à son compte utilisateur. Si vous sélectionnez un utilisateur avec une autorisation Administrator ACL ou OA, la page est grisée, désactive l'accès aux autorisations de lame et d'interconnexion et les sélectionne toutes.

Pour les cas où HP SIM est utilisé, Onboard Administrator peut s'intégrer à HP SIM et employer des utilisateurs HP SIM pour faciliter une connexion unique de HP SIM vers Onboard Administrator. Pour plus d'informations, reportez-vous à la section Intégration de HP SIM.

Comptes utilisateur basés sur les rôles

Les comptes utilisateur basés sur les rôles sur le module Onboard Administrator servent deux objectifs : contrôler les fonctions auxquelles un utilisateur a accès sur le module Onboard Administrator, ainsi que contrôler les autorisations qu'un compte utilisateur temporaire adopte sur iLO lorsque la connexion automatique est utilisée.

Deux aspects majeurs de comptes utilisateur basés sur les rôles sont proposés sur le module Onboard Administrator : les autorisations de baie et un niveau de privilège d'utilisateur. Les autorisations de baie déterminent les baies auxquelles l'utilisateur peut accéder. Les autorisations de baie sont sélectionnées au cours de la création du compte utilisateur et permettent d'accéder à des baies de périphérique, baies d'interconnexion ou baies de module Onboard Administrator spécifiques. Le niveau de privilège détermine les fonctions d'administration que l'utilisateur est autorisé à exécuter. Le niveau de privilège d'un utilisateur peut être administrateur, opérateur ou utilisateur.

Un utilisateur doté d'un niveau de privilège administrateur et d'une autorisation sur les baies OA dans le boîtier se voit automatiquement octroyer un accès intégral à toutes les baies et peut exécuter toute fonction sur le boîtier ou les baies, notamment gestion de comptes utilisateur et configuration du boîtier. Un opérateur ayant uniquement une autorisation sur les baies OA peut configurer le boîtier, mais ne peut pas gérer les utilisateurs ou les paramètres de sécurité, comme il ne peut pas accéder aux autres baies. Un utilisateur doté d'une autorisation sur les baies OA peut visualiser uniquement les paramètres de configuration, mais ne peut pas modifier ces derniers. Des comptes utilisateur peuvent être créés avec plusieurs autorisations de baies, mais le même niveau de privilège s'applique à toutes ces baies.

Des comptes utilisateur configurés pour autoriser l'accès à des baies de périphériques peuvent être créés pour des administrateurs de serveur. Si l'utilisateur se connecte au module Onboard Administrator, il reçoit des informations sur les baies de serveur autorisées. Si l'utilisateur sélectionne l'iLO de l'interface utilisateur graphique Web du module Onboard Administrator, il est automatiquement connecté à cet iLO à l'aide d'un compte utilisateur temporaire avec son niveau de privilège. Les utilisateurs d'iLO avec le niveau de privilège administrateur ont le contrôle complet, notamment la modification des comptes utilisateur. Les opérateurs ont un contrôle intégral sur l'alimentation du serveur et les consoles. Les utilisateurs ont un accès minimum en lecture seule sur les informations du serveur. L'utilisation de cette fonction de connexion unique simplifie grandement la supervision de plusieurs serveurs à partir de l'interface utilisateur Web Onboard Administrator.

Les autorisations sur les modules d'interconnexion sont légèrement différentes. La connexion automatique n'est pas prise en charge pour les modules d'interconnexion, mais tous les niveaux d'utilisateur ont accès au lien de console de supervision pour les baies d'interconnexion pour lesquelles ils ont une autorisation. Les administrateurs et opérateurs peuvent utiliser les boutons virtuels du module Onboard Administrator pour contrôler l'alimentation et le voyant d'UID sur le module d'interconnexion. Les utilisateurs peuvent uniquement visualiser l'état et les informations sur le module d'interconnexion.

Exemples

La section ci-dessous présente des exemples de scénarios de supervision dans un environnement c-Class et les comptes utilisateur qui peuvent être créés pour fournir le niveau de sécurité approprié.

Scénario 1 : un membre d'une organisation requiert un accès complet aux serveurs dans les baies 1-8 pour visualiser les journaux, contrôler l'alimentation et utiliser la console distante. L'utilisateur n'a pas l'autorisation de gérer les paramètres du module Onboard Administrator. Le compte utilisateur permettant d'obtenir ce niveau de sécurité a un niveau d'accès administrateur et une autorisation sur les baies de serveur 1-8. Ainsi, l'utilisateur n'a pas l'autorisation sur les baies Onboard Administrator ou les baies d'interconnexion.

Scénario 2 : un membre d'une organisation a besoin de ports pour gérer les ports sur deux modules d'interconnexion dans les baies 3 et 4. Cette personne doit connaître quels ports sur la carte sont mappés à certains serveurs. Cependant, cette personne ne doit pas pouvoir gérer les serveurs. Le compte utilisateur permettant d'obtenir ce niveau de sécurité a un niveau d'accès utilisateur, une autorisation sur toutes les baies de serveur et une autorisation sur les baies d'interconnexion 3 et 4. Cependant, cet utilisateur ne peut pas contrôler l'alimentation ou le voyant d'UID pour les modules d'interconnexion ou les lames. Pour contrôler l'alimentation ou le voyant d'UID sur les modules d'interconnexion, le privilège de l'utilisateur doit être opérateur. Pour empêcher cet utilisateur d'effectuer des opérations de serveur telles que le contrôle de l'alimentation ou des opérations de console, le compte est limité uniquement aux autorisations sur les baies pour les baies d'interconnexion 3 et 4.

Utilisateurs locaux

New (Nouveau) : pour ajouter un nouvel utilisateur au boîtier sélectionné, cliquez sur le bouton **New**. L'écran Add Local User (Ajout d'utilisateur local) s'affiche.

REMARQUE : 30 comptes utilisateur au maximum peuvent être configurés en mode FIPS OFF, alors que 21 comptes utilisateur au maximum peuvent être configurés en mode FIPS ON ou DEBUG. La limite du nombre d'utilisateurs maximum inclut des comptes réservés tels que les comptes administrateur et Virtual Connect.

Edit (Modifier) : sélectionnez un utilisateur (vous ne pouvez en sélectionner qu'un seul) en cochant la case située en regard du nom de l'utilisateur. Pour modifier les paramètres de l'écran Edit Local User (Modification d'utilisateur local), cliquez sur **Edit** (Modifier).

Delete (Supprimer) : sélectionnez un ou plusieurs utilisateurs à supprimer en cochant la case en regard du nom de chaque utilisateur. Pour supprimer les comptes, cliquez sur **Delete**. Si vous essayez de supprimer le dernier compte administrateur restant, un avertissement d'alerte indique qu'un compte administrateur doit exister et l'action de suppression est annulée.

Ajout d'un utilisateur local

Champ	Valeur possible	Description
Username (Nom d'utilisateur)	De 1 à 40 caractères, y compris tous les caractères alphanumériques, le tiret (-) et le trait de soulignement (_).	30 comptes utilisateur au maximum peuvent être configurés en mode FIPS OFF, alors que 21 comptes utilisateur au maximum peuvent être configurés en mode FIPS ON ou DEBUG. La limite du nombre d'utilisateurs maximum inclut des comptes réservés tels que les comptes administrateur et Virtual Connect. Les noms d'utilisateur ALL (non-respect de la casse), ADMINISTRATOR (respect de la casse), switch1, switch2, switch3, switch4, switch5, switch6, switch7, switch8, ldapuser, nobody, tbmuser_, vcmuser et vcmuser_ sont réservés ; vous ne pouvez pas les utiliser. Le nom d'utilisateur peut commencer par une lettre et est sensible à la différence majuscules-minuscules.
Password (Mot de passe)	En mode FIPS ON/DEBUG, ou en mode FIPS OFF avec mots de passe robustes activés, le mot de passe doit contenir au moins un caractère parmi trois des quatre types de caractères. Les quatre types sont majuscules, minuscules, caractères numériques et caractères non alphanumériques. La longueur du mot de passe doit être comprise entre 8 et 40 caractères. En mode FIPS OFF, le mot de passe peut comporter n'importe quel caractère imprimable, et le mot de passe doit comprendre entre 3 et 40 caractères.	Mot de passe associé à l'utilisateur.
Password Confirm (Confirmation de mot de passe)	La longueur et les caractères du mot de passe doivent être conformes aux règles de mot de passe décrites dans la ligne précédente.	Mot de passe associé à l'utilisateur. Cette valeur doit correspondre à la valeur entrée dans Password (Mot de passe).

Pour enregistrer les paramètres, cliquez sur **Add User** (Ajouter utilisateur). L'écran Edit Local User (Modification de l'utilisateur local) s'affiche.

REMARQUE : Des doublons d'utilisateur dotés du même nom et d'une casse différente peuvent être ajoutés. Veillez à sélectionner l'utilisateur approprié lors de l'attribution ou de la modification de l'autorisation d'un utilisateur.

Modification de l'utilisateur local

Informations utilisateur

Champ	Valeur possible	Description
Password (Mot de passe)	En mode FIPS ON/DEBUG, ou en mode FIPS OFF avec mots de passe robustes activés, le mot de passe doit contenir au moins un caractère parmi trois des quatre types de caractères. Les quatre types sont majuscules, minuscules, caractères numériques et caractères non alphanumériques. La longueur du mot de passe doit être comprise entre 8 et 40 caractères. En mode FIPS OFF avec mots de passe robustes désactivés, le mot de passe peut comporter n'importe quel caractère imprimable, et le mot de passe doit comprendre entre 3 et 40 caractères.	Mot de passe associé à l'utilisateur.
Password Confirm (Confirmation de mot de passe)	La longueur et les caractères du mot de passe doivent être conformes aux règles de mot de passe décrites dans la ligne précédente.	Mot de passe associé à l'utilisateur. Cette valeur doit correspondre à la valeur entrée dans Password (Mot de passe).
Full Name (Nom complet)	De 0 à 20 caractères, incluant tous les caractères alphanumériques, le tiret (-), le trait de soulignement (_) et l'espace.	Nom complet de l'utilisateur. Tous les utilisateurs peuvent modifier leur propre nom complet.
Contact	De 0 à 20 caractères, incluant tous les caractères alphanumériques, le tiret (-), le trait de soulignement (_) et l'espace.	Informations de contact pour le compte utilisateur. Les informations de contact peuvent être le nom d'une personne, un numéro de téléphone ou toute autre information utile. Tous les utilisateurs peuvent modifier leurs propres informations de contact.

Le champ Username (Nom d'utilisateur) ne peut pas être modifié sur l'écran Edit Local User (Modification de l'utilisateur local).

Privilege Level (Niveau de privilège)

Classification du compte	Capacités	Nom du compte / Niveau de privilège	Baies sélectionnées pour ce compte
Administrateur	• Toutes les commandes • Compte local, non LDAP • Seul compte restant après une réinitialisation du module Onboard Administrator sur les réglages par défaut (le compte conserve le mot de passe Administrateur configuré)	Administrateur / administrateur	Tous

Classification du compte	Capacités	Nom du compte / Niveau de privilège	Baies sélectionnées pour ce compte
	• Le mot de passe du compte Administrateur peut être réinitialisé sur le réglage usine par défaut via le port série du module Onboard Administrator à l'aide de l'option `L` de récupération du mot de passe en cas de perte. • Peut télécharger, ajouter et effacer une clé SSH. Cette clé ne fonctionne qu'avec le compte Administrateur		
Administrateur OA	• Toutes les commandes • Permet d'accéder à tous les aspects du boîtier HP BladeSystem et du module Onboard Administrator, y compris la configuration, les mises à jour de microprogramme, la gestion des utilisateurs et la réinitialisation sur les paramètres par défaut	nom d'utilisateur / administrateur	Baies OA (sélection automatique de toutes les baies)
Administrateur	• Peut exécuter toute opération sur les baies de périphériques et d'interconnexion autorisées, y compris alimentation virtuelle et accès console • permission d'administrateur sur iLO de périphérique	nom d'utilisateur / administrateur	Aucune baie OA et uniquement les baies de périphériques et d'interconnexion sélectionnés
Opérateur OA	• Permet d'accéder à tous les aspects du boîtier HP BladeSystem et du module Onboard Administrator, à l'exception de la supervision des utilisateurs	nom d'utilisateur / opérateur	Baies OA ; peut avoir d'autres baies sélectionnées, mais capacités opérateur sur celles-ci*
Opérateur	• Peut exécuter toute opération sur les baies de périphériques et d'interconnexion autorisées, y compris alimentation virtuelle et accès console • permission d'opérateur sur iLO de périphérique	nom d'utilisateur / opérateur	Baies de périphériques et d'interconnexion sélectionnées

Classification du compte	Capacités	Nom du compte / Niveau de privilège	Baies sélectionnées pour ce compte
Utilisateur OA	• Peut afficher l'état et les informations du boîtier • Peut afficher l'historique de la CLI	nom d'utilisateur / utilisateur	Baies OA et possibilité d'avoir d'autres baies sélectionnées, mais les possibilités des autres baies sont définies dans l'utilisateur
Utilisateur	• Peut afficher l'état et les informations des baies sélectionnées • Peut afficher l'historique de la CLI • Peut définir le mot de passe de son propre compte • Peut définir les informations de contact utilisateur de son propre compte • Peut afficher des commandes CLI	nom d'utilisateur / utilisateur	Aucune baie OA et quelques baies de périphériques et d'interconnexion

* Les fonctionnalités EBIPA et VLAN permettent d'accéder à l'ensemble des baies pour un opérateur OA.

User Enabled (Utilisateur activé) doit être sélectionné pour activer le compte utilisateur. Si un compte utilisateur est désactivé, toutes les sessions ouvertes pour ce compte sont terminées (déconnectées).

Modification de niveau de privilège

Si un niveau de privilège de compte utilisateur est modifié, toutes les sessions ouvertes pour ce compte utilisateur sont terminées (déconnectées). L'utilisateur doit se connecter à nouveau après la modification de niveau de privilège.

Cases à cocher

L'activation de la case à cocher de la baie de base du périphérique n'autorise pas l'utilisateur à accéder à un serveur double densité sans vérifier au préalable les options A et B pour cette baie. Activez uniquement A ou B pour une baie de périphériques si vous restreignez l'autorisation à un serveur unique dans une lame de serveur à double densité plus élevée.

Autorisations utilisateur

Case à cocher	Description
Onboard Administrator Bays (Baies Onboard Administrator)	Donne les autorisations utilisateur pour toutes les baies Onboard Administrator. Si le niveau de privilège utilisateur est Administrator, alors les options All Device Bays (Toutes les baies de périphérique) et All Interconnect Bays (Toutes les baies d'interconnexion) sont sélectionnées automatiquement si l'option Onboard Administrator Bays (Baies Onboard Administrator) est sélectionnée et toutes les cases à cocher sont grisées.
All Device Bays (Toutes les baies de périphérique)	Donne les autorisations utilisateur pour toutes les baies de périphérique.

Case à cocher	Description
Selected Device Bays (Baies de périphériques sélectionnées)	Donne les autorisations utilisateur pour uniquement les baies de périphériques sélectionnées.
All Interconnect Bays (Toutes les baies d'interconnexion)	Donne les autorisations utilisateur pour toutes les baies d'interconnexion.
Selected Interconnect Bays (Baies d'interconnexion sélectionnées)	Donne les autorisations utilisateur pour uniquement les baies d'interconnexion sélectionnées.

Pour enregistrer les modifications, cliquez sur **Update User**.

Modification des informations de certificat des utilisateurs locaux

Lorsque l'authentification à deux facteurs est activée, vous devez posséder un certificat utilisateur pour vous connecter au module Onboard Administrator. Les utilisateurs dotés de droits d'administrateur peuvent télécharger ou mapper un certificat valide vers un utilisateur sélectionné.

REMARQUE : Lorsque le module Onboard Administrator fonctionne en mode FIPS, la longueur minimale de la clé RSA ne doit pas être inférieure à 2 048 bits, et l'algorithme de hachage de la signature doit être SHA1, SHA-224, SHA-256, SHA-384 ou SHA-512.

Vous pouvez utiliser deux méthodes pour télécharger des certificats en vue de les utiliser dans le module HP BladeSystem Onboard Administrator :

- Collez le contenu du certificat dans la zone de texte et sélectionnez **Upload** (Télécharger).
- Collez l'URL complète du certificat dans le champ URL et sélectionnez **Apply** (Appliquer).

Une fois le certificat téléchargé avec succès, l'empreinte SHA1 du certificat utilisateur apparaît.

Si vous disposez déjà d'un certificat mappé sur un compte, l'empreinte SHA1 du certificat apparaît. Tout utilisateur doté de droits d'administrateur peut supprimer son certificat et télécharger un nouveau certificat utilisateur. Lorsque votre certificat expire et est renouvelé, tant que le certificat renouvelé a le même nom d'objet que celui qui est expiré, vous n'avez pas besoin de télécharger le certificat renouvelé vers le module Onboard Administrator.

Paramètres de mot de passe

Cet écran permet de mettre en œuvre des fonctions de mot de passe robuste. Seuls les administrateurs dotés d'une autorisation Onboard Administrator sont autorisés à gérer les mots de passe robustes.

Pour activer cette fonction, sélectionnez **Enable Strong Passwords** (Activer les mots de passe robustes). Pour enregistrer le paramètre, cliquez sur **Apply** (Appliquer).

REMARQUE : Cette option ne peut pas être désactivée en mode FIPS ON/DEBUG.

Avec le mode FIPS ON/DEBUG ou les mots de passe robustes activés, le mot de passe doit contenir trois des quatre types de caractères répertoriés dans le tableau suivant.

Type de caractères	Description
Majuscules	Un caractère majuscule compris dans le jeu de caractères A à Z.
Minuscules	Un caractère minuscule compris dans le jeu de caractères a à z.

Type de caractères	Description
Numérique	Un caractère numérique compris dans le jeu de caractères 0 à 9.
Non-alphanumérique	Tout caractère imprimable qui n'est pas un espace ou un caractère alphanumérique.

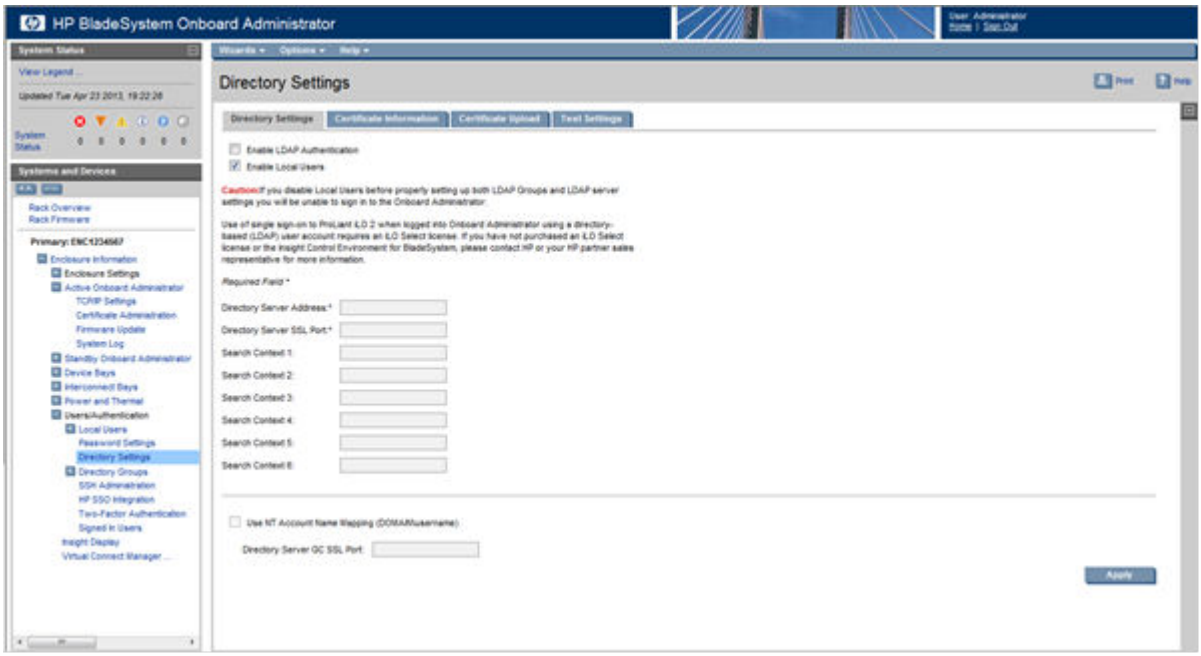
Avec le mode FIPS OFF et les mots de passe robustes désactivés, la longueur minimum du mot de passe peut être comprise entre 3 et 40 caractères. Si la longueur minimum du mot de passe n'est pas configurée, elle contient par défaut trois caractères. En mode FIPS ON/DEBUG, ou avec le mode FIPS OFF et les mots de passe robustes activés, la longueur minimum du mot de passe (et par défaut) est de huit caractères. Pour enregistrer le paramètre de longueur minimum du mot de passe, cliquez sur **Apply** (Appliquer).

Écran Directory Settings

LDAP est un protocole d'accès aux annuaires d'information. Bien que le protocole LDAP soit basé sur la norme X.500, il est bien plus simple que cette norme. LDAP prend également en charge le TCP/IP et est un protocole ouvert.

REMARQUE : La fonction LDAP du module Onboard Administrator prend en charge Microsoft® Active Directory à l'aide de l'attribut `memberOf`. Novell eDirectory est également pris en charge avec l'attribut `groupMembership`. OpenLDAP n'est pas pris en charge.

Utilisez l'écran Directory Settings (Paramètres d'annuaire) pour définir l'accès aux annuaires du boîtier sélectionné.



- **Enable LDAP Authentication** (Activer l'authentification LDAP) : cochez cette case pour permettre à un serveur d'annuaire d'authentifier une connexion d'utilisateur.
- **Enable Local Users** (Activer les utilisateurs locaux) : cochez cette case pour permettre à un utilisateur de se connecter via un compte utilisateur local et non un compte d'annuaire.

- **Search Context** (Contexte de recherche) : spécifiez un à six contextes de recherche. Un contexte de recherche est un filtre de recherche ou un raccourci vers un annuaire commun, définissant le début de la recherche de l'utilisateur d'annuaire à l'emplacement spécifié. En spécifiant un contexte de recherche, les utilisateurs n'ont pas à indiquer leurs DN complets lors de la connexion. Un DN peut être long, et les utilisateurs peuvent ne pas connaître leurs DN ou peuvent avoir des comptes dans différents contextes d'annuaire. Le module Onboard Administrator tente de contacter le service d'annuaire par DN, puis applique les contextes de recherche dans l'ordre, en commençant par `Search Context 1` et continue à travers tous les contextes de recherche suivants jusqu'à la réussite.

  - **Exemple 1** :

    Supposons que vous êtes `user1`. Si vous entrez le contexte de recherche `ou=OU1,dc=hp,dc=com`, vous pouvez vous connecter en tant que `user1` au lieu de `cn=user1,ou=OU1,dc=hp,dc=com`.

  - **Exemple 2** :

    Supposons que les contextes de recherche suivants sont définis :

    - Contexte de recherche 1 : `ou=OU1,dc=hp,dc=com`
    - Contexte de recherche 2 : `ou=OU2,ou=OU1,dc=hp,dc=com`

    Si deux utilisateurs disposent du même nom commun `user1` dans deux contextes de recherche, et que leurs mots de passe sont identiques, lorsque l'utilisateur tente de se connecter, le module Onboard Administrator contacte `cn=user1,ou=OU1,dc=hp,dc=com`.

    Si les mots de passe sont différents et qu'un utilisateur fournit le mot de passe de l'utilisateur dans `OU2`, le module Onboard Administrator utilise DN `cn=user1,ou=OU1,dc=hp,dc=com`, mais il sera rejeté parce que le mot de passe ne correspond pas. La prochaine connexion sera tentée avec `cn=user1,ou=OU2,ou=OU1,dc=hp,dc=com`, avec succès.

Le contexte de recherche est également applicable aux groupes d'annuaires, qui sont utiles lorsque des groupes imbriqués LDAP sont configurés. Lorsque vous spécifiez le contexte de recherche pour un groupe d'annuaire LDAP, le contexte exact n'est pas nécessaire. Par exemple, si un emplacement de groupe est ou=OU2,ou=OU1,dc=hp,dc=com, le contexte de recherche de niveau supérieur ou=OU1,dc=hp,dc=com peut être utilisé pour localiser ce groupe. Cette fonction permet de contourner la limite de longueur des contextes de recherche. Pour plus d'informations sur les groupes imbriqués, consultez la section « Groupes d'annuaires » (Groupes d'annuaires à la page 341).

Champ	Valeur possible	Description
Directory Server Address (Adresse du serveur d'annuaire)	Adresse IPv4 : ###.###.###.### où ### est compris dans une plage de 0 à 255 ou nom DNS du serveur d'annuaire ou nom du domaine. Adresse Ipv6 : ####:####:####:####:####:####:####:####, où #### est compris entre 0 et FFFF. Une version comprimée de la même adresse IPv6 est également prise en charge.	Adresse IP, nom DNS ou nom du domaine du service d'annuaire. Ce champ est obligatoire.

Champ	Valeur possible	Description
Directory Server SSL Port (Port SSL du serveur d'annuaire)	1 à 65535	Port utilisé pour les communications LDAP. Le port 636 est le port LDAP SSL standard. Ce champ est obligatoire.
Search Context 1 (Contexte de recherche 1)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Premier chemin de recherche utilisé pour localiser l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.
Search Context 2 (Contexte de recherche 2)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Deuxième chemin de recherche utilisé pour localiser l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.
Search Context 3 (Contexte de recherche 3)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Troisième chemin de recherche utilisé pour localiser l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.
Search Context 4 (Contexte de recherche 4)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Quatrième chemin de recherche utilisé pour repérer l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.
Search Context 5 (Contexte de recherche 5)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Cinquième chemin de recherche utilisé pour repérer l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.
Search Context 6 (Contexte de recherche 6)	Tous les caractères à l'exception des guillemets ("). Limité à 127 caractères.	Sixième chemin de recherche utilisé pour repérer l'utilisateur lorsque celui-ci tente de s'authentifier via les services d'annuaire. Le chemin est également utilisé pour rechercher un groupe d'imbrication LDAP.

- **Use NT Account Name Mapping (DOMAIN\username)** (Utiliser le mappage de noms de comptes NT (DOMAINE\nom d'utilisateur)) : cochez cette case pour permettre le mappage de noms NT. Ce champ permet aux utilisateurs de se connecter en utilisant le format NT `domaine\nom_utilisateur`. Le module Onboard Administrator peut être configuré en option pour rechercher le Catalogue mondial du serveur d'annuaire et localiser les informations de l'utilisateur authentifié et des groupes autorisés associés. Le port GC SSL standard du serveur d'annuaire est 3269. Ce champ est facultatif et, s'il reste vierge, le catalogue mondial n'est pas utilisé.

REMARQUE : Si le mappage de noms de comptes NT est utilisé avec le catalogue mondial et que le contexte de recherche n'est pas assez restrictif, ou bien que le nom du domaine n 'est pas spécifié, le module Onboard Administrator peut associer l'utilisateur authentifié à un compte utilisateur qui a le même nom dans un domaine différent. L'utilisateur authentifié recevrait alors l'autorisation de l'utilisateur dans l'autre domaine. Pour éviter toute ambigüité lors de la connexion de l'utilisateur LDAP, sélectionnez les contextes de recherche ou fournissez le nom du domaine.

REMARQUE : Si le mappage de noms de comptes NT est utilisé avec le catalogue mondial et ne peut pas être résolu avec un utilisateur unique, l'utilisateur n'est pas autorisé à accéder au module Onboard Administrator. Cela peut se produire avec des contextes de recherche qui ne sont pas assez restrictifs et si plusieurs comptes ayant le même nom existent dans différents domaines. Pour éviter toute ambigüité, sélectionnez les contextes de recherche.

Cliquez sur **Apply** (Appliquer) pour enregistrer les paramètres.

REMARQUE : Les règles de mot de passe appliquées sur les serveurs LDAP pourraient être différentes des règles de mot de passe appliquées pour les comptes utilisateur locaux. Assurez-vous que les deux ensembles de règles adhèrent aux politiques de sécurité.

Onglet Directory Certificate Information

Cet écran affiche les informations détaillées de tous les certificats LDAP qui sont actuellement en vigueur sur le module Onboard Administrator.

Rangée	Description
Issued To (Émis pour)	Organisation à laquelle le certificat a été émis
Issued by (Émis par)	Autorité de certification qui a émis le certificat
Valid from (Valide à partir de)	Date à partir de laquelle le certificat est valide
Valid until (Valide jusqu'à)	Date à laquelle le certificat expire
Serial Number (Numéro de série)	Numéro de série attribué au certificat par l'autorité de certification
Version	Numéro de version du certificat actuel
MD5 Fingerprint (Empreinte MD5)	Validation de l'authenticité, intégrée dans le certificat
SHA1 Fingerprint (Empreinte SHA1)	Validation de l'authenticité, intégrée dans le certificat
Public Key (Clé publique)	Nom de la clé publique

Cliquez sur **Remove** (Retirer) au-dessous du certificat LDAP à retirer du boîtier.

Téléchargement d'un certificat

Les certificats protègent les informations d'identification des utilisateurs contre les attaques de l'intercepteur (man-in-the-middle). Si les certificats ne sont pas chargés sur le module Onboard Administrator, il est possible qu'un intercepteur affiche les informations d'identification LDAP de toute personne qui se connecte au module Onboard Administrator. Onboard Administrator accepte plusieurs certificats de contrôleur de domaine, qui peuvent être téléchargés via l'onglet Certificate Upload (Téléchargement de certificat) sous les paramètres d'annuaire (Directory Settings).

Pour télécharger un certificat :

1. Obtenez le certificat du contrôleur de domaine en ouvrant un navigateur et en entrant l'adresse suivante :

   https://<domain controller>:636

   où *domain controller* est l'adresse IP pour votre contrôleur de domaine de réseau.

2. Lorsqu'invité à accepter un certificat :

   - Si vous utilisez Internet Explorer 6, cliquez sur **View Certificate** (Afficher le certificat).
   - Si vous utilisez Internet Explorer 7 ou version ultérieure, cliquez sur **Continue to this website (not recommended)** (Continuer vers ce site Web [non recommandé]), puis cliquez sur **Certificate Error** (Erreur de certificat) dans la barre d'adresse supérieure. Cliquez sur **View Certificate** (Afficher le certificat).

3. Cliquez sur l'onglet **Details**, puis sur le bouton **Copy to File** (Copier dans fichier).

4. Dans la liste d'options d'exportation, sélectionnez Base-64 encoded x.509 (.CER). Fournissez un nom et un emplacement pour le fichier, puis terminez l'exécution de l'assistant de téléchargement de certificat.

5. Repérez le fichier de certificat exporté et renommez-le avec une extension .txt (par exemple, dccert.txt). Ouvrez le fichier dans un éditeur de texte, puis copiez le contenu entier vers le Presse-papiers. Les éléments suivants sont un exemple d'un fichier de certificat exporté :

   ```
   -----BEGIN CERTIFICATE-----

   MIIFxDCCBKygAwIBAgIKJWUSwAAAAAAAAjANBgkqhkiG9w0BAQUFADBVMRMwEQYK

   CZImiZPyLGQBGRYDY29tMRIwEAYKCZImiZPyLGQBGRYCaHAxFzAVBgoJkiaJk/Is

   ZAEZFgdhdGxkZW1vMREwDwYDVQQDEwh3aW5kb3pDQTAeFw0wNjA4MjIyMDIzMTFa

   Fw0wNzA4MjIyMDIzMTFaMCAxHjAcBgNVBAMTFXdpbmRvei5hdGxkZW1vLmhwLmNv

   bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAy4zeh3iXydUAWKVHIDsxLJ6B

   aRuVT9ZhkL5NQHIDeRjumsgc/jHSERDmHuyoY/qbF7JMhJ9Lh9QQHUg8QfEYsC1y

   qTvgisrZeHtvmrmecvSxZm27b4Bj5XYN0VYcrwqKnH7X/tVhmwqGls7/YZyahNU1

   lGB2OjoCq5eJxX+Ybx0CAwEAAaOCA00wggNJMAsGA1UdDwQEAwIFoDBEBgkqhkiG

   9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4D

   …output truncated…

   -----END CERTIFICATE-----
   ```

6. Revenez au module Onboard Administrator, collez le contenu du certificat dans la fenêtre, puis cliquez sur **Upload** (Charger).

Onglet Directory Certificate Upload

Cet écran permet de télécharger un certificat LDAP vers le module Onboard Administrator afin d'établir une relation de confiance avec le serveur LDAP. Vous pouvez télécharger au maximum quatre certificats.

Vous pouvez utiliser deux méthodes pour télécharger des certificats en vue de les utiliser dans le module HP BladeSystem Onboard Administrator :

- Collez le contenu du certificat dans la zone de texte et sélectionnez **Upload** (Télécharger).
- Collez l'URL complète du certificat dans le champ URL et sélectionnez **Apply** (Appliquer).

Onglet Directory Test Settings

L'onglet **Test Settings** (Paramètres de test) permet aux administrateurs de module Onboard Administrator de s'assurer que les informations de configuration fournies autorisent l'accès d'utilisateurs d'annuaire au module Onboard Administrator et aux ressources dans le boîtier. L'onglet **Test Settings** s'applique uniquement aux paramètres actuels. Par conséquent, après avoir apporté des modifications à l'onglet **Directory Settings**, vous devez cliquer sur le bouton **Apply** (Appliquer), puis sélectionner l'onglet **Test Settings**.

Utilisez l'onglet **Test Settings** pour exécuter et signaler les tests. Lorsque la page de l'onglet apparaît initialement, elle contient une liste de tests avec l'état actuel `Not Run` (Non exécuté). Pour exécuter les tests, cliquez sur **Test Settings**. Les tests sont exécutés dans l'ordre dans lequel ils apparaissent. Les tests prennent fin lorsqu'une erreur se produit. Pour effectuer les tests d'authentification de l'utilisateur et d'autorisation d'utilisateur, vous devez entrer un nom d'utilisateur et un mot de passe dans la section **Directory Test Controls** (Contrôles de test d'annuaire).

Les tests suivants sont effectués dans l'ordre fourni.

- **Overall Test Status (État de test global)**

  L'état de test global est un agrégat de tous les tests exécutés. La valeur sera `Not Run` (Non exécuté), `Passed` (Réussi) ou `Failed` (Échec). Si un des tests individuels échoue, l'état est `Failed`.

- **Ping Directory Server (Test ping sur un serveur d'annuaire)**

  Un simple test de commande ping est effectué après avoir vérifié l'existence d'une adresse IP ou d'un nom de domaine valide pour le serveur d'annuaire. Le test de commande ping envoie un maximum de quatre paquets ping au serveur d'annuaire et renvoie un état de réussite ou d'échec.

  - Un test réussi indique que le module Onboard Administrator peut établir un chemin d'accès réseau au serveur d'annuaire.
  - Un test qui échoue indique que le module Onboard Administrator peut établir un chemin d'accès réseau au serveur d'annuaire. L'administrateur doit vérifier le nom d'hôte ou l'adresse IP.

- **Directory Server IP Address (Adresse IP du serveur d'annuaire)**

  Si la configuration LDAP spécifie une adresse IP au lieu d'un DNS, ce test vérifie alors que l'adresse IP est une adresse IPv4 valide. Sinon, le test renvoie l'état `Not Run` (Non exécuté).

  - Un test réussi indique que l'adresse IP enregistrée pour le serveur d'annuaire est une adresse IPv4 valide.
  - Un test qui échoue indique que l'adresse IP enregistrée pour le serveur d'annuaire n'est pas une adresse IPv4 valide. L'administrateur doit vérifier l'adresse IP entrée et corriger l'adresse IP.

- **Directory Server DNS Name (Nom DNS du serveur d'annuaire)**

  Le test de recherche DNS détermine si le module Onboard Administrator peut résoudre le nom de domaine du serveur LDAP. Si la configuration du serveur LDAP utilise des adresses IP au lieu d'un nom DNS, ce test renvoie l'état `Not Run` (Non exécuté).

- Un test réussi indique que le module Onboard Administrator est en mesure de résoudre le nom d'hôte de serveur d'annuaire à l'aide du nom de domaine.
- Un test qui échoue indique que le module Onboard Administrator ne peut pas résoudre le nom d'hôte de serveur d'annuaire. L'administrateur doit vérifier que le nom d'hôte de serveur d'annuaire est correct et que le nom d'hôte est correct pour le serveur d'annuaire.

- **Connect to Directory Server (Connexion au serveur d'annuaire)**

  Ce test essaie une connexion à l'adresse IP de serveur d'annuaire spécifiée et au port de service.

  - Un test réussi indique que le module Onboard Administrator peut établir une connexion au serveur d'annuaire au nom d'hôte ou à l'adresse spécifié(e) et au numéro de port spécifié. Un test réussi indique que le service réseau est disponible ; le service d'annuaire est exécuté et disponible au serveur d'annuaire et au port spécifiés.
  - Un test qui échoue indique que le module Onboard Administrator ne peut pas établir de connexion au serveur d'annuaire. Le test qui échoue indique que le service réseau n'est pas disponible. L'administrateur doit vérifier le nom d'hôte ou l'adresse et le numéro de port.

- **Connect using SSL (Connexion via SSL)**

  Ce test vérifie que le serveur d'annuaire fournit le service d'annuaire sur une connexion SSL.

  - Un test réussi indique que le module Onboard Administrator peut établir une connexion SSL au nom d'hôte de serveur d'annuaire ou à l'adresse IP et au port. Le service réseau est disponible comme connexion SSL sécurisée.
  - Un test qui échoue indique que le service réseau n'est pas disponible comme connexion SSL sécurisée et que le module Onboard Administrator n'autorise pas ce type de connexion. L'administrateur doit identifier un serveur d'annuaire qui prend en charge des connexions SSL, ou doit reconfigurer le serveur d'annuaire pour utiliser des connexions SSL.

- **Certificate of Directory Server (Certificat du serveur d'annuaire)**

  Si le certificat SSL du serveur d'annuaire a été chargé sur le module Onboard Administrator, utilisez ce test pour vérifier que le certificat fourni par le serveur d'annuaire correspond au certificat actuel enregistré sur le module Onboard Administrator. Si le certificat SSL du serveur d'annuaire n'a pas été chargé, ce test ne peut alors pas être effectué.

  - Un test réussi indique que le module Onboard Administrator était en mesure de valider le certificat de serveur d'annuaire en tenant compte des certificats enregistrés sur le module Onboard Administrator pour le serveur d'annuaire spécifié.
  - Un test qui échoue indique que le certificat de serveur d'annuaire enregistré sur le module Onboard Administrator ne correspond pas au certificat fourni sur la connexion SSL.

- **Authentification de l'utilisateur**

  Ce test essaie de connecter l'utilisateur à l'annuaire à l'aide du nom d'utilisateur et du mot de passe fournis dans la section **Directory Test Controls**. Si l'authentification de l'utilisateur échoue à l'aide du nom d'utilisateur et du mot de passe fournis, chaque contexte de recherche est envisagé. Si un contexte de recherche commence par le caractère @, alors le DN utilisé pour la connexion est le nom de recherche concaténé au nom d'utilisateur entré. Sinon, le DN de recherche utilisé pour la connexion est construit comme suit :

`cn=<nom_utilisateur>,<contexte_recherche>`. Le résultat de ce test identifie le contexte de recherche permettant l'authentification de l'utilisateur.

- **User Authorization (Autorisation utilisateur)**

  Après l'authentification et la connexion d'un utilisateur au module Onboard Administrator, le groupe d'annuaire configuré auquel l'utilisateur appartient est identifié. Un utilisateur peut appartenir à plusieurs groupes d'annuaire, donc le groupe d'annuaire qui donne le plus de privilèges à l'utilisateur est identifié.

  - Un test réussi indique le groupe d'annuaire avec les niveaux de privilège les plus élevés pour l'utilisateur authentifié.
  - Un test qui échoue indique que l'utilisateur authentifié ne dispose d'aucune autorisation sur le module Onboard Administrator car l'utilisateur n'appartient à aucun des groupes d'annuaire configurés.

Test Log (Journal de test)

Il s'agit d'un journal d'exécution des détails associés aux tests qui ont été exécutés et des résultats de ces tests.

Directory Test Controls (Contrôles des tests d'annuaire)

Le nom d'utilisateur et le mot de passe sont envoyés au serveur LDAP pour authentification avant l'exécution des tests d'authentification d'utilisateur et d'autorisation d'utilisateur. Le module Onboard Administrator limite la longueur du nom d'utilisateur et du mot de passe comme indiqué. Des exigences de configuration sont définies par le serveur LDAP ; les limites de longueur imposées par le serveur LDAP peuvent être plus restreintes que les limites imposées par le module Onboard Administrator.

- Nom d'utilisateur : accepte de 0 à 256 caractères.
- Mot de passe : accepte de 0 à 1024 caractères.

Groupes d'annuaires

L'accès au boîtier peut être accordé en utilisant LDAP. Pour utiliser le serveur LDAP, vous devez créer des comptes d'annuaire.

L'écran Directory Groups affiche les groupes d'annuaires actuels qui ont été ajoutés au boîtier de la connexion principale. Vous pouvez ajouter des groupes d'utilisateurs à tous les boîtiers. Vous pouvez modifier et supprimer des groupes d'utilisateurs uniquement du boîtier de connexion principale. Pour utiliser les services LDAP, vous devez ajouter au moins un groupe d'annuaires.

Colonne	Description
Case à cocher	Permet de sélectionner un groupe d'annuaires pour modification ou suppression.
Group Name (Nom de groupe)	De 1 à 255 caractères. Contient les mêmes caractères que les contextes de recherche. Le nom de groupe est utilisé pour déterminer l'appartenance à un groupe d'utilisateurs LDAP. Le nom de groupe doit correspondre à l'une des cinq propriétés suivantes d'un groupe d'annuaires : le nom, le nom unique, le nom commun, le nom d'affichage ou le nom de compte SAM. Pour les groupes imbriqués, la correspondance est basée sur `objectSid` (un attribut qui spécifie l'identifiant de sécurité du groupe). Le nom unique est recommandé pour spécifier uniquement le groupe LDAP. Si le module Onboard Administrator est configuré pour rechercher le port GC et si un nom unique n'est pas utilisé,

Colonne	Description
	alors une correspondance incorrecte dans plusieurs domaines peut se produire pour entraîner une autorisation involontaire.
Privilege Level (Niveau de privilège)	Utilisé pour déterminer les fonctions d'administration que l'utilisateur est autorisé à exécuter. Le niveau de privilège d'un utilisateur peut être administrateur, opérateur ou utilisateur.
Description	De 0 à 58 caractères, incluant les caractères alphanumériques, le tiret (-), le trait de soulignement (_) et l'espace. Description du groupe LDAP, une version plus lisible du nom de groupe, ou d'autres informations utiles.

- **New** (Nouveau) : cliquez sur le bouton **New** pour ajouter un nouvel groupe d'annuaires au boîtier sélectionné. Vous pouvez ajouter un maximum de 30 groupes d'annuaires. L'écran Add LDAP Group (Ajouter un groupe LDAP) s'affiche.
- **Edit** (Modifier) : sélectionnez un groupe d'annuaires à modifier en activant la case à cocher en regard du nom du groupe. Pour modifier les paramètres dans l'écran Edit LDAP Group (Modification du groupe LDAP), cliquez sur **Edit** (Modifier).
- **Delete** (Supprimer) : sélectionnez le groupe d'annuaires à supprimer en activant la case à cocher en regard du nom du groupe. Pour supprimer le groupe, cliquez sur **Delete** (Supprimer).

Prise en charge de groupe LDAP imbriqué

Lorsque vous utilisez Microsoft Active Directory, vous pouvez placer un ou plusieurs groupes dans un autre groupe. Les groupes qui sont contenus dans un autre groupe sont appelés des groupes imbriqués. Le groupe qui contient des groupes imbriqués est appelé un groupe d'imbrication. L'avantage des groupes imbriqués est de pouvoir connecter les utilisateurs d'un groupe imbriqué au module Onboard Administrator si leur groupe d'imbrication est correctement configuré. Par exemple, supposons que `group2` est imbriqué dans `group1`. Les utilisateurs de `group2` sont autorisés à se connecter au module Onboard Administrator si le groupe LDAP parent (`group1`) est ajouté au module Onboard Administrator et peut être trouvé en utilisant l'un des contextes de recherche. Le contexte de la recherche ne se limite pas à l'emplacement exact : si le chemin de contexte de recherche est élevé dans l'arborescence de l'annuaire LDAP, la recherche de sous-arbre est utilisée. Le module Onboard Administrator ne prend en charge que le type de groupe de sécurité. Le type de groupe de distribution n'est pas pris en charge.

Ajout d'un groupe LDAP

Informations de groupe

REMARQUE : Un maximum de 30 groupes d'annuaires peut être ajouté.

Champ	Valeur possible	Description
Group Name (Nom de groupe)	1 à 255 caractères ; tous les caractères sauf les guillemets ("). Le premier caractère du nom de groupe doit être un caractère alphanumérique.	Le nom de groupe est utilisé pour déterminer l'appartenance à un groupe d'utilisateurs LDAP. Le nom de groupe doit correspondre à l'une des cinq propriétés suivantes d'un groupe d'annuaires : le nom, le nom unique, le nom commun, le nom d'affichage ou le nom de compte SAM. Le nom unique est recommandé pour spécifier

Champ	Valeur possible	Description
		uniquement le groupe LDAP. Si le module Onboard Administrator est configuré pour rechercher le port GC et si un nom unique n'est pas utilisé, alors une correspondance incorrecte dans plusieurs domaines peut se produire pour entraîner une autorisation involontaire.
Description	De 0 à 58 caractères, incluant tous les caractères alphanumériques, le tiret (-), le trait de soulignement (_) et l'espace.	Peut contenir une version plus lisible du nom de groupe, ainsi que d'autres informations utiles.

Privilege Level (Niveau de privilège)

Classification du compte	Capacités	Nom du compte / Niveau de privilège	Baies sélectionnées pour ce compte
Administrateur	• Toutes les commandes • Compte local, non LDAP • Seul compte restant après une réinitialisation du module Onboard Administrator sur les réglages par défaut (le compte conserve le mot de passe Administrateur configuré) • Le mot de passe du compte Administrateur peut être réinitialisé sur le réglage usine par défaut via le port série du module Onboard Administrator à l'aide de l'option `L` de récupération du mot de passe en cas de perte. • Peut télécharger, ajouter et effacer une clé SSH. Cette clé ne fonctionne qu'avec le compte Administrateur	Administrateur / administrateur	Tous
Administrateur OA	• Toutes les commandes • Permet d'accéder à tous les aspects du boîtier HP BladeSystem et du module Onboard Administrator, y compris la configuration, les mises à jour de microprogramme, la gestion des utilisateurs et la réinitialisation sur	nom d'utilisateur / administrateur	Baies OA (sélection automatique de toutes les baies)

Classification du compte	Capacités	Nom du compte / Niveau de privilège	Baies sélectionnées pour ce compte
	les paramètres par défaut		
Administrateur	• Peut exécuter toute opération sur les baies de périphériques et d'interconnexion autorisées, y compris alimentation virtuelle et accès console • permission d'administrateur sur iLO de périphérique	nom d'utilisateur / administrateur	Aucune baie OA et uniquement les baies de périphériques et d'interconnexion sélectionnés
Opérateur OA	• Permet d'accéder à tous les aspects du boîtier HP BladeSystem et du module Onboard Administrator, à l'exception de la supervision des utilisateurs	nom d'utilisateur / opérateur	Baies OA ; peut avoir d'autres baies sélectionnées, mais capacités opérateur sur celles-ci*
Opérateur	• Peut exécuter toute opération sur les baies de périphériques et d'interconnexion autorisées, y compris alimentation virtuelle et accès console • permission d'opérateur sur iLO de périphérique	nom d'utilisateur / opérateur	Baies de périphériques et d'interconnexion sélectionnées
utilisateur OA	• Peut afficher l'état et les informations du boîtier • Peut afficher l'historique de la CLI	nom d'utilisateur / utilisateur	Baies OA et possibilité d'avoir d'autres baies sélectionnées, mais les possibilités des autres baies sont définies dans l'utilisateur
Utilisateur	• Peut afficher l'état et les informations des baies sélectionnées • Peut afficher l'historique de la CLI • Peut définir le mot de passe de son propre compte • Peut définir les informations de contact utilisateur de son propre compte • Peut afficher des commandes CLI	nom d'utilisateur / utilisateur	Aucune baie OA et quelques baies de périphériques et d'interconnexion

* Les fonctionnalités EBIPA et VLAN permettent d'accéder à l'ensemble des baies pour un opérateur OA.

Autorisations de groupe

Case à cocher	Description
Onboard Administrator Bays (Baies Onboard Administrator)	Donne les autorisations utilisateur pour toutes les baies Onboard Administrator. Si le niveau de privilège utilisateur est Administrator, alors les options All Device Bays (Toutes les baies de périphérique) et All Interconnect Bays (Toutes les baies d'interconnexion) sont sélectionnées automatiquement si l'option Onboard Administrator Bays (Baies Onboard Administrator) est sélectionnée et toutes les cases à cocher sont grisées.
All Device Bays (Toutes les baies de périphérique)	Donne les autorisations utilisateur pour toutes les baies de périphérique.
Selected Device Bays (Baies de périphériques sélectionnées)	Donne les autorisations utilisateur pour uniquement les baies de périphériques sélectionnées.
All Interconnect Bays (Toutes les baies d'interconnexion)	Donne les autorisations utilisateur pour toutes les baies d'interconnexion.
Selected Interconnect Bays (Baies d'interconnexion sélectionnées)	Donne les autorisations utilisateur pour uniquement les baies d'interconnexion sélectionnées.

Pour enregistrer les paramètres, cliquez sur **Add Group** (Ajouter groupe).

Modification d'un groupe LDAP

Informations de groupe

Champ	Valeur possible	Description
Group Name (Nom de groupe)	1 à 255 caractères ; tous les caractères sauf les guillemets ("). Le premier caractère du nom de groupe doit être un caractère alphanumérique.	Le nom de groupe est utilisé pour déterminer l'appartenance à un groupe d'utilisateurs LDAP. Le nom de groupe doit correspondre à l'une des cinq propriétés suivantes d'un groupe d'annuaires : le nom, le nom unique, le nom commun, le nom d'affichage ou le nom de compte SAM. Le nom unique est recommandé pour spécifier uniquement le groupe LDAP. Si le module Onboard Administrator est configuré pour rechercher le port GC et si un nom unique n'est pas utilisé, alors une correspondance incorrecte dans plusieurs domaines peut se produire pour entraîner une autorisation involontaire.
Description	De 0 à 58 caractères, incluant tous les caractères alphanumériques, le tiret (-), le trait de soulignement (_) et l'espace.	Peut contenir une version plus lisible du nom de groupe, ainsi que d'autres informations utiles.

Privilege Level (Niveau de privilège)

Classification du compte	Capacités	Nom du compte / Niveau de privilège	Baies sélectionnées pour ce compte
Administrateur	• Toutes les commandes	Administrateur / administrateur	Tous

Classification du compte	Capacités	Nom du compte / Niveau de privilège	Baies sélectionnées pour ce compte
	• Compte local, non LDAP • Seul compte restant après une réinitialisation du module Onboard Administrator sur les réglages par défaut (le compte conserve le mot de passe Administrateur configuré) • Le mot de passe du compte Administrateur peut être réinitialisé sur le réglage usine par défaut via le port série du module Onboard Administrator à l'aide de l'option `L` de récupération du mot de passe en cas de perte. • Peut télécharger, ajouter et effacer une clé SSH. Cette clé ne fonctionne qu'avec le compte Administrateur		
Administrateur OA	• Toutes les commandes • Permet d'accéder à tous les aspects du boîtier HP BladeSystem et du module Onboard Administrator, y compris la configuration, les mises à jour de microprogramme, la gestion des utilisateurs et la réinitialisation sur les paramètres par défaut	nom d'utilisateur / administrateur	Baies OA (sélection automatique de toutes les baies)
Administrateur	• Peut exécuter toute opération sur les baies de périphériques et d'interconnexion autorisées, y compris alimentation virtuelle et accès console • permission d'administrateur sur iLO de périphérique	nom d'utilisateur / administrateur	Aucune baie OA et uniquement les baies de périphériques et d'interconnexion sélectionnés
Opérateur OA	• Permet d'accéder à tous les aspects du boîtier HP BladeSystem et du module Onboard Administrator, à l'exception de la supervision des utilisateurs	nom d'utilisateur / opérateur	Baies OA ; peut avoir d'autres baies sélectionnées, mais capacités opérateur sur celles-ci*

Classification du compte	Capacités	Nom du compte / Niveau de privilège	Baies sélectionnées pour ce compte
Opérateur	• Peut exécuter toute opération sur les baies de périphériques et d'interconnexion autorisées, y compris alimentation virtuelle et accès console • permission d'opérateur sur iLO de périphérique	nom d'utilisateur / opérateur	Baies de périphériques et d'interconnexion sélectionnées
Utilisateur OA	• Peut afficher l'état et les informations du boîtier • Peut afficher l'historique de la CLI	nom d'utilisateur / utilisateur	Baies OA et possibilité d'avoir d'autres baies sélectionnées, mais les possibilités des autres baies sont définies dans l'utilisateur
Utilisateur	• Peut afficher l'état et les informations des baies sélectionnées • Peut afficher l'historique de la CLI • Peut définir le mot de passe de son propre compte • Peut définir les informations de contact utilisateur de son propre compte • Peut afficher des commandes CLI	nom d'utilisateur / utilisateur	Aucune baie OA et quelques baies de périphériques et d'interconnexion

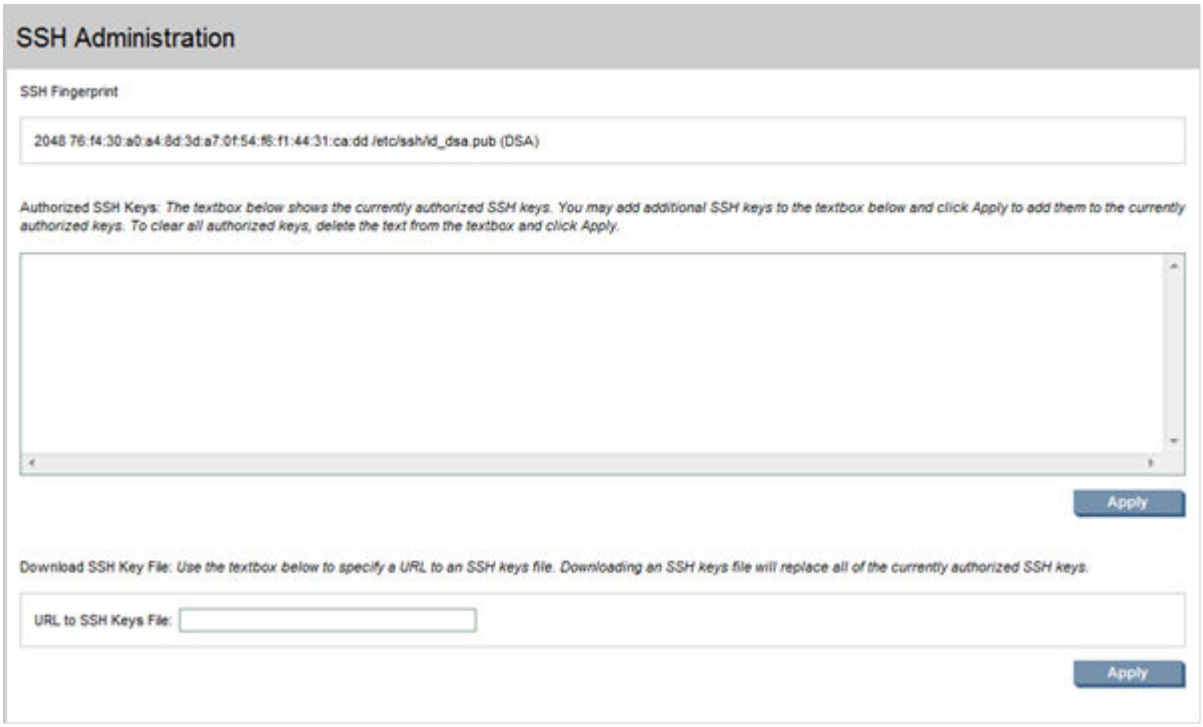
* Les fonctionnalités EBIPA et VLAN permettent d'accéder à l'ensemble des baies pour un opérateur OA.

Autorisations de groupe

Case à cocher	Description
Onboard Administrator Bays (Baies Onboard Administrator)	Donne les autorisations utilisateur pour toutes les baies Onboard Administrator. Si le niveau de privilège utilisateur est Administrator, alors les options All Device Bays (Toutes les baies de périphérique) et All Interconnect Bays (Toutes les baies d'interconnexion) sont sélectionnées automatiquement si l'option Onboard Administrator Bays (Baies Onboard Administrator) est sélectionnée et toutes les cases à cocher sont grisées.
All Device Bays (Toutes les baies de périphérique)	Donne les autorisations utilisateur pour toutes les baies de périphérique.
Selected Device Bays (Baies de périphériques sélectionnées)	Donne les autorisations utilisateur pour uniquement les baies de périphériques sélectionnées.
All Interconnect Bays (Toutes les baies d'interconnexion)	Donne les autorisations utilisateur pour toutes les baies d'interconnexion.
Selected Interconnect Bays (Baies d'interconnexion sélectionnées)	Donne les autorisations utilisateur pour uniquement les baies d'interconnexion sélectionnées.

Pour enregistrer les paramètres, cliquez sur **Update Group** (Mettre à jour groupe).

Administration SSH


SSH Administration
SSH Fingerprint
2048 76:f4:30:a0:a4:8d:3d:a7:0f:54:f6:f1:44:31:ca:dd /etc/ssh/id_dsa.pub (DSA)
Authorized SSH Keys: The textbox below shows the currently authorized SSH keys. You may add additional SSH keys to the textbox below and click Apply to add them to the currently authorized keys. To clear all authorized keys, delete the text from the textbox and click Apply.
Apply
Download SSH Key File: Use the textbox below to specify a URL to an SSH keys file. Downloading an SSH keys file will replace all of the currently authorized SSH keys.
URL to SSH Keys File:
Apply

Cette page indique le propriétaire de chaque clé SSH autorisée et permet d'ajouter de nouvelles clés.

SSH Fingerprint (Empreinte SSH) : partie de la clé publique d'une paire de clés publiques/privées.

Authorized SSH Keys (Clés SSH autorisées) : répertorie en détail les données de clés SSH autorisées. Le propriétaire est toujours l'administrateur. Pour ajouter des clés SSH autorisées supplémentaires, entrez la clé SSH dans la zone de texte, puis cliquez sur **Apply** (Appliquer). Pour désactiver toutes les clés SSH autorisées, supprimez tout le texte dans la zone de texte, puis cliquez sur **Apply** (Appliquer).

Download SSH Key File (Télécharger le fichier de clés SSH) : dans le champ URL to SSH Keys File (URL vers le fichier de clés SSH), entrez l'emplacement du fichier de clés publiques et cliquez sur **Apply** (Appliquer) pour télécharger. Toutes les clés SSH actuellement autorisées sont remplacées lorsque le fichier de clés SSH est téléchargé. Chaque clé est associée au compte administrateur.

REMARQUE : Lorsque le module Onboard Administrator fonctionne en mode FIPS, la longueur minimale de la clé RSA ne doit pas être inférieure à 2 048 bits, et l'algorithme de hachage de la signature doit être SHA1, SHA-224, SHA-256, SHA-384 ou SHA-512.

Versions SSH et SSL prises en charge

Version Onboard Administrator	Version SSL	Version SSH
v1.20	openssl – 0.9.7k	openssh – 4.2p1
v2.00	openssl – 0.9.7l	openssh – 4.2p1
v2.30 - v2.60	openssl – 0.9.7m	openssh – 4.4p1

Version Onboard Administrator	Version SSL	Version SSH
v3.00	openssl – fips-1.2 openssl – 0.9.8j	openssh – 5.1p1
v3.10	openssl – fips-1.2 openssl – 0.9.8n	openssh – 5.1p1
v 3.20	openssl – fips-1.2 openssl – 0.9.8n	openssh – 5.1p1
v3.50 - v3.55	openssl – 0.9.8r	openssh – 5.8p2
v3.56 - v3.71	openssl – 0.9.8w	openssh – 5.8p2
v4.01 - 4.02	openssl – 0.9.8y	openssh – 5.8p2
v4.11 - v4.22	openssl – fips-2.0.5 openssl – 1.0.1e	openssh – 6.2p2
v4.30	openssl – fips-2.0.5 openssl – 1.0.1f	openssh – 6.2p2
v4.40 - v4.50	openssl – fips 2.0.5 openssl – 1.0.1h	openssh – 6.2p2

Intégration de HP SSO

Le module HP BladeSystem Onboard Administrator prend en charge SSO avec des applications approuvées, telles que HP OneView ou HP SIM. La fonction HP SSO permet de se connecter à une application de gestion approuvée, puis d'accéder automatiquement à tout périphérique géré sur lequel le certificat SSO est installé. Pour configurer SSO afin de travailler via HP SSO :

1. Définissez le mode de certification SSO sur ON (Activé). Dans l'écran HP SSO Integration (Intégration de HP SSO), sélectionnez **Trust by Certificate** (Certifier par certificat) dans le menu déroulant **Trust mode** (Mode de certification).

REMARQUE : Lorsque le mode de confiance est désactivé, la tentative de connexion ponctuelle HP SSO échoue et vous devez entrer les informations d'identification Onboard Administrator pour vous connecter.

HP SSO Integration
Print
Help
Settings
Certificate Information
Certificate Upload
HP SSO Trust Mode: The trust mode setting determines the manner in which the Onboard Administrator will validate a single sign-on attempt from an HP management server.
Trust mode:
Trust By Certificate
Apply

2. Sur l'écran HP SSO Integration, sélectionnez l'onglet **Certificate Upload** (Chargement de certificat).
3. Chargez un certificat, à l'aide de l'une des méthodes suivantes :
   - Collez le contenu du certificat dans la zone de texte, puis cliquez sur **Upload** (Charger).

- Entrez l'adresse IP du système HP SSO qui gérera le boîtier, puis cliquez sur **Apply** (Appliquer).

REMARQUE : Onboard Administrator 4.12 ou version ultérieure contient une prise en charge de l'application HP SSO afin de déterminer les exigences minimum du certificat SSO.

Authentification à deux facteurs

Onglet Two-Factor Authentication Settings

REMARQUE : Le module Onboard Administrator doit être configuré en mode Virtual Connect avant de pouvoir activer l'authentification à deux facteurs lors de l'utilisation du Virtual Connect Manager et de la fonction Two-Factor Authentication.

Lorsque l'authentification à deux facteurs est activée, seuls les utilisateurs possédant un certificat utilisateur valide sont autorisés à se connecter au module Onboard Administrator. Un certificat utilisateur valide est signé par une Autorité de certification approuvée et est mappé sur l'utilisateur concerné sur le module Onboard Administrator.

Pour activer l'utilisation de l'authentification à deux facteurs pour l'authentification d'un utilisateur durant la connexion, sélectionnez **Enable Two-Factor Authentication** (Mettre en œuvre l'authentification à deux facteurs). Lorsque l'authentification à deux facteurs est activée, l'accès SSH et Telnet est désactivé par défaut. La désactivation de l'authentification à deux facteurs ne réactive pas automatiquement SSH et Telnet. Vous devez accéder à l'écran Network Access (Accès réseau), puis sélectionner **Enable Secure Shell** (Activer Secure Shell) et **Enable Telnet** (Activer Telnet).

Pour permettre au module Onboard Administrator de vérifier auprès de l'Autorité de certification que le certificat utilisé a été ajouté à la liste de révocation de certificats (CRL), sélectionnez **Check for Certificate Revocation** (Contrôler la révocation de certificat). Si le certificat figure sur la liste CRL, la connexion est refusée.

Champ Certificate Owner (Propriétaire du certificat)

Vous pouvez configurer le module Onboard Administrator afin d'utiliser le nom de principe de l'utilisateur dans le SAN en sélectionnant SAN ou pour utiliser le nom d'objet de certificat en sélectionnant Subject (Objet) lors de l'authentification des utilisateurs d'annuaire avec un serveur d'annuaires.

Pour enregistrer les paramètres, cliquez sur **Apply** (Appliquer).

Pour plus d'informations sur la configuration de l'authentification à deux facteurs pour des comptes de groupe LDAP et d'utilisateur local, consultez la section « Création d'autorités de certification et configuration de l'autorisation à deux facteurs pour comptes de groupe LDAP et d'utilisateur local »

(Création d'autorités de certification et configuration de l'autorisation à deux facteurs pour comptes de groupe LDAP et d'utilisateur local à la page 404).

Onglet Certificate Information de l'authentification à deux facteurs

Cet écran affiche tous les certificats du serveur Insight Remote Control approuvés par le module Onboard Administrator. Douze certificats au maximum peuvent être téléchargés vers le module Onboard Administrator.

Rangée	Description
Certificate Version (Version du certificat)	Numéro de version du certificat actuel
Issuer Organization (Organisation émettrice)	Nom de l'organisation qui a émis le certificat
Issuer Organization Unit (Unité de l'organisation émettrice)	Nom de l'unité organisationnelle qui a émis le certificat
Issued by (Émis par)	Autorité de certification qui a émis le certificat
Subject Organization (Organisation d'objet)	Nom de l'objet
Issued To (Émis à)	Organisation à laquelle le certificat a été émis
Valid From (Valide à partir de)	Date à partir de laquelle le certificat est valide
Valid Upto (Valide jusqu'à)	Date à laquelle le certificat expire
Serial Number (Numéro de série)	Numéro de série attribué au certificat par l'autorité de certification
Extension Count (Nombre d'extensions)	Nombre d'extensions dans le certificat
MD5 Fingerprint (Empreinte MD5)	Ce champ peut être utilisé pour valider l'authenticité du certificat
SHA1 Fingerprint (Empreinte SHA1)	Ce champ peut être utilisé pour valider l'authenticité du certificat.

Pour supprimer un certificat existant, cliquez sur **Remove**.

Onglet Certificate Upload de l'authentification à deux facteurs

Pour activer l'authentification à deux facteurs, téléchargez au moins un certificat valide appartenant à une CA vers le module Onboard Administrator.

Vous pouvez utiliser deux méthodes pour télécharger des certificats en vue de les utiliser dans le module HP BladeSystem Onboard Administrator :

- Collez le contenu du certificat dans la zone de texte et sélectionnez **Upload** (Télécharger).
- Collez l'URL complète du certificat dans le champ URL et sélectionnez **Apply** (Appliquer).

Signed In Users

Cet écran affiche toutes les sessions en cours connectées au module Onboard Administrator. Cet écran est uniquement disponible pour les administrateurs ayant un accès au module Onboard Administrator. L'administrateur peut mettre fin aux sessions, désactiver des utilisateurs et supprimer des utilisateurs à partir de cet écran.

Current Session (Session actuelle) : ce tableau répertorie la session créée lors de votre connexion au module Onboard Administrator.

Other Sessions (Autres sessions) : ce tableau répertorie les autres utilisateurs connectés au module Onboard Administrator.

Colonne	Description
Case à cocher	Utilisé pour sélectionner un ou tous les utilisateurs.
Username (Nom d'utilisateur)	Nom de l'utilisateur connecté au boîtier.
IP Address (Adresse IP)	Adresse IP du compte utilisateur. L'adresse IP de la session peut être une adresse liée au boîtier si elle a la forme 169.254.1.x. Ces sessions sont créées par d'autres boîtiers liés. L'exécution d'une suppression, désactivation ou fin de session sur un utilisateur ayant une adresse IP de boîtier lié peut mettre fin aux sessions de liaison de boîtier d'autres utilisateurs. Pour les connexions KVM et série, le champ d'adresse IP affiche Local.
Age (Âge)	Durée, en jours, heures, minutes et secondes, de la connexion du compte utilisateur.
Idle Time (Temps d'inactivité)	Durée d'inactivité, en jours, heures, minutes et secondes, du compte utilisateur connecté.
User Type (Type d'utilisateur)	Type de l'utilisateur connecté au boîtier. Les valeurs possibles sont Local, LDAP et HP SSO.
Session Type (Type de session)	Type de session de l'utilisateur connecté. Les valeurs possibles sont Web, SSH, Telnet, KVM, Serial (Série) et Factory Diagnostics (Diagnostics usine).
OA Module (Module OA)	Module Onboard Administrator auquel l'utilisateur est connecté. Les valeurs possibles sont Active (Actif) et Standby (Mode Standby).

Delete Users (Supprimer utilisateurs) : sélectionnez un ou plusieurs utilisateurs à supprimer en cochant la case située en regard du nom de l'utilisateur, puis cliquez sur **Delete Users** (Supprimer utilisateurs). Vous ne pouvez pas supprimer votre propre compte ou le compte Administrateur intégré.

Disable Users (Désactiver utilisateurs) : sélectionnez un ou plusieurs utilisateurs à désactiver en cochant la case située en regard du nom de l'utilisateur, puis cliquez sur **Disable Users** (Désactiver utilisateurs). Vous ne pouvez pas désactiver votre propre compte ou le compte Administrateur intégré.

Terminate Sessions (Mettre fin aux sessions) : sélectionnez un ou plusieurs utilisateurs dont vous souhaitez mettre fin aux sessions en cochant la case située en regard du nom de l'utilisateur, puis cliquez sur **Terminate Sessions** (Mettre fin aux sessions). Vous ne pouvez pas mettre fin à votre propre session.

Onglet Session Options

Cet écran permet de spécifier la durée de validité d'une session utilisateur s'il n'y a aucune activité. Les sessions sont vérifiées toutes les cinq minutes pour voir si elles ont été inactives pendant la durée spécifiée par l'administrateur système. Toute session inactive pendant la durée spécifiée est supprimée du système.

Session Timeout (Expiration de session) : le nombre de minutes avant qu'une session inactive devienne non valide. Le paramètre Session Timeout peut être toute valeur comprise entre 10 et 1440 (24 heures). Pour désactiver Session Timeout, réglez-le à 0. La valeur par défaut pour Session Timeout est 1440. Après avoir saisi une valeur de Session Timeout, cliquez sur **Apply** (Appliquer).

Insight Display

Tous les utilisateurs d'interface du module Onboard Administrator peuvent accéder aux écrans Insight Display en sélectionnant Insight Display dans l'affichage en arborescence ou dans l'affichage Rack Overview (Vue d'ensemble du rack).

L'onglet Security (Sécurité) peut verrouiller les boutons Insight Display, définir un code PIN, ainsi qu'activer une protection par code PIN.

REMARQUE : Lorsque le module Onboard Administrator fonctionne en mode FIPS ON/DEBUG, la protection par code PIN ne peut pas être désactivée.

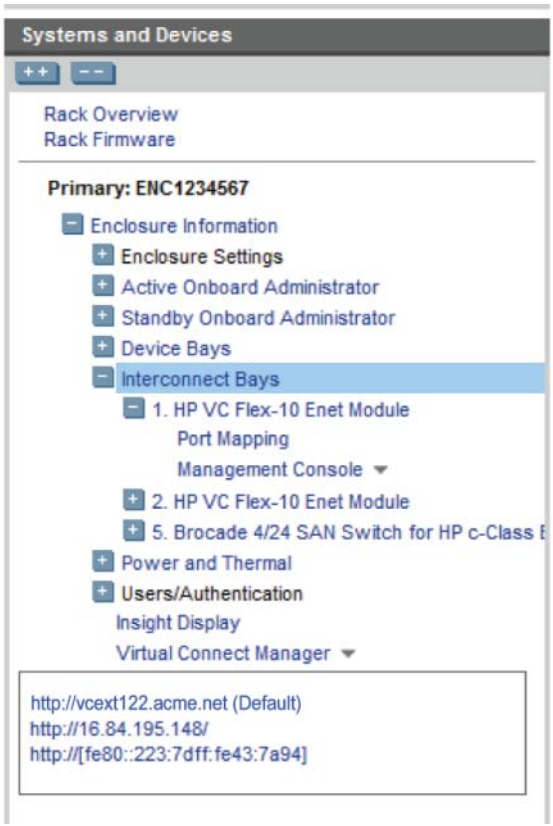
L'onglet User Note (Remarque de l'utilisateur) permet la saisie de texte de remarque modifiable.

L'onglet Background (Arrière-plan) permet le téléchargement d'une image bitmap 320x240 Windows comme image d'arrière-plan pour les remarques de l'utilisateur.

L'onglet Chat Mode (Mode Chat) permet à un administrateur de lancer une conversation avec un utilisateur devant le boîtier à l'aide du module Insight Display.

Virtual Connect Manager

Le lien Virtual Connect Manager du menu d'arborescence démarre Virtual Connect Manager dans une nouvelle fenêtre. Pour afficher les liens disponibles d'adresses VCM (IPv4 et IPv6), cliquez sur la flèche vers le bas à côté du lien. Lorsque la prise en charge de lien FQDN est activée et que certaines exigences de configuration DNS sont remplies, une adresse basée sur le nom de domaine complet s'affiche en tant que valeur par défaut, comme indiqué dans la figure suivante. Pour plus d'informations sur l'activation de la prise en charge du lien FQDN, consultez la page « Accès réseau ».



Pour plus d'informations sur l'utilisation de Virtual Connect Manager, consultez le *Manuel de l'utilisateur de HP Virtual Connect Manager*.

Intégration iLO

Le HP BladeSystem Onboard Administrator s'intègre au système iLO de chaque lame de serveur et permet une authentification directe (pass-through) à partir du module Onboard Administrator. Tout comme l'interface CLI, le HP BladeSystem Onboard Administrator peut prendre en charge jusqu'à 4 utilisateurs connectés simultanément au système iLO via l'authentification directe. Pour établir la connexion au port iLO de la lame de serveur, cliquez sur le lien **iLO**. Si le compte utilisateur est configuré sur le système iLO et correspond à celui du module Onboard Administrator, l'utilisateur peut alors accéder à l'interface du système iLO qui apparaîtra sur le même écran.

Dépendances IP du réseau de supervision

Le port de supervision des modules Onboard Administrator permet aux clients externes de se connecter via le module Onboard Administrator aux iLO et aux processeurs de supervision d'interconnexion configurés pour utiliser le réseau de supervision interne des modules Onboard Administrator.

Le microprogramme du module Onboard Administrator lie le trafic client au boîtier entre le port de supervision et le réseau de supervision du boîtier interne si l'adresse IP de destination ne correspond pas au module Onboard Administrator. Le module Onboard Administrator crée une entrée de table d'itinéraire pour l'adresse IP iLO de chaque serveur dans un boîtier. Ceci permet au module Onboard Administrator de conduire des communications IP avec ce module iLO. Ces entrées de table de routage iLO permettent de configurer chaque réseau iLO dans un sous-réseau différent du module Onboard Administrator. Chaque iLO est configuré avec une passerelle valide sur son sous-réseau qui

est accessible via la connexion au port de supervision externe des modules Onboard Administrator. Les routeurs sont requis sur le réseau connecté au port de supervision Onboard Administrator pour fournir plusieurs sous-réseaux et passerelles sur le réseau de supervision. L'utilisation de sous-réseaux différents pour essayer d'isoler les iLO et la supervision Onboard Administrator ne permet pas une isolation parfaite de ces réseaux.

9 Utilisation de l'interface de ligne de commande

Présentation de la ligne de commande

L'interface CLI du module Onboard Administrator est disponible depuis le port série, le port de supervision, le port de service ou l'option c3000 KVM Module du module Onboard Administrator. Cette interface fournit l'accès à toutes les commandes et informations du module Onboard Administrator.

L'utilisateur CLI doit fournir un nom d'utilisateur/mot de passe valide pour se connecter au module Onboard Administrator. L'interface CLI est disponible à la fois pour les comptes utilisateur locaux et les utilisateurs LDAP. L'authentification à deux facteurs n'est pas disponible pour l'interface CLI.

Accéder à l'interface CLI du module Onboard Administrator depuis le port de supervision Ethernet ou le port de service du module Onboard Administrator nécessite l'activation des protocoles telnet ou SSH sur le module Onboard Administrator.

Accéder à l'interface CLI du module Onboard Administrator depuis le port série du module c3000 KVM Module ou Onboard Administrator est toujours possible quel que soit le paramètre du protocole telnet ou SSH.

Le port série du module Onboard Administrator doit être utilisé pour la récupération par flashage du microprogramme du module Onboard Administrator ou pour la récupération du mot de passe administrateur oublié.

La vitesse de port série du module Onboard Administrator est définie sur 9600, N, 8, 1.

Pour plus d'informations sur l'interface de ligne de commande, reportez-vous au document *HP BladeSystem Onboard Administrator Command Line Interface User Guide* (Manuel de l'utilisateur de l'interface de ligne de commande HP BladeSystem Onboard Administrator).

Installation du module Onboard Administrator à l'aide de l'interface CLI

1. Connectez-vous à l'interface CLI du module Onboard Administrator à l'aide du port série, du port de supervision, du port de service ou de l'option c3000 KVM Module.
2. Connectez-vous au module Onboard Administrator avec le compte utilisateur Administrator et le mot de passe OA dogtag.
3. Définissez le nom du module Onboard Administrator : "SET OA NAME 1 <nom>".
4. Si un module Onboard Administrator redondant est présent, définissez le nom sur : "SET OA NAME 2 <nom>".
5. Configurez l'adresse IP du module Onboard Administrator
   a. Indiquez s'il faut utiliser l'adresse IP OA1/OA2 ou l'adresse IP du boîtier.
   b. Configurez l'adresse IP OA1 comme adresse statique ou DHCP. Exemple d'adresse statique : "SET IPCONFIG STATIC 1 <adresse_ip><masque_réseau>"

6. Si un module Onboard Administrator redondant est présent : "SET IPCONFIG STATIC 2 <adresse ip> <masque_réseau>".
7. Définissez la passerelle du module Onboard Administrator : "SET OA GATEWAY 1 <adresse ip>".
8. Si un module Onboard Administrator redondant est présent : "SET OA GATEWAY 2 <adresse ip>".
9. Définissez l'adresse IP d'iLO : "SET EBIPA SERVER <adresse ip> <masque_réseau>". Allouez chaque adresse IP nécessaire (jusqu'à 32 adresses IP statiques consécutives).
10. Si une passerelle est présente sur le réseau de gestion, définissez la passerelle du iLO sur l'adresse IP : SET EBIPA SERVER GATEWAY <adresse ip>.
11. Démarrez EBIPA POUR iLO : "ENABLE EBIPA SERVER".
12. Finalisez le paramétrage en fonction des besoins. Le Manuel de l'utilisateur de l'interface CLI indique les valeurs par défaut de boîtier pour chaque paramètre.

Configuration d'adresses IP iLO c-Class

Chaque configuration par défaut d'usine iLO c-Class active les paramètres réseau DHCP. Pour utiliser l'iLO avec un réseau DHCP, connectez le port de supervision Onboard Administrator à un réseau avec un serveur DHCP et un module Onboard Administrator et tous les processeurs de supervision iLO et modules d'interconnexion de prise en charge comme Virtual Connect récupèrent des adresses IP du serveur DHCP.

Pour configurer chaque iLO pour les adresses IP statiques, il existe cinq possibilités. Utilisez le module Onboard Administrator pour configurer une adresse IP pour chaque iLO à l'aide d'EBIPA. Cela permet l'adressage de l'iLO à l'aide de TCP/IP afin que les paramètres réseau puissent être reconfigurés. Le PC client doit être configuré pour accéder temporairement à ces adresses IP iLO pour les possibilités 2-4 ci-dessous.

Possibilité 1 à l'aide d'EBIPA :

La configuration de chaque iLO avec une adresse IP à l'aide d'EBIPA fournit une configuration réseau fixe, notamment l'adresse IP, masque de réseau et passerelle, basée sur la baie de boîtier où le serveur est installé. Le nouvel iLO obtient l'adresse IP pour cette baie sans configuration supplémentaire exigée.

Possibilité 2 à l'aide de l'interface GUI OA :

Connectez-vous à l'interface graphique du module OA avec un compte doté de privilèges d'administrateur et de permissions de baie sur le module iLO correspondant. Sélectionnez le lien **iLO** sur le serveur souhaité pour établir une authentification unique à l'interface graphique Web iLO. Sélectionnez **Administration | Network Settings** (Administration | Paramètres réseau). Modifiez iLO en DHCP désactivé et entrez l'adresse IP souhaitée, le masque de sous-réseau et la passerelle. Sélectionnez **Apply** (Appliquer) et l'iLO est alors configuré avec une adresse IP statique. Répétez ces étapes pour chaque iLO. Une fois que tous les iLO dans le boîtier possèdent des adresses IP statiques configurées, désactivez le paramètre EBIPA pour les serveurs.

Possibilité 3 à l'aide de l'interface CLI OA :

Connectez-vous à l'interface CLI du module OA avec un compte doté de privilèges d'administrateur et de permissions de baie sur le module iLO correspondant. Exécutez la commande `connect server X` où *X* est le numéro de la baie contenant l'iLO à configurer. Utilisez l'interface SMASH/CLP iLO pour définir l'iLO sur le masque de sous-réseau d'adresse IP et la passerelle souhaités. Cela réinitialise les paramètres réseau iLO aux valeurs configurées. Répétez ces étapes pour chaque iLO. Une fois que tous les iLO dans le boîtier possèdent des adresses IP statiques configurées, désactivez le paramètre EBIPA pour les serveurs.

Possibilité 4 à l'aide de scripts RIBCL iLO :

Créez un script xml RIBCL unique pour configurer les paramètres réseau iLO sur les valeurs souhaitées pour chaque iLO. Copiez ces scripts vers un serveur HTTP, FTP ou TFTP qui soit accessible par le module Onboard Administrator.

Connectez-vous à l'interface CLI du module OA avec un compte doté de privilèges d'administrateur et de permissions de baie sur le module iLO correspondant. Exécutez la commande `hponcfg X Y` où *X* est le numéro de la baie contenant la carte iLO à configurer et *Y* est le chemin réseau du serveur HTTP, FTP ou TFTP vers le fichier de script (par exemple, hponcfg 2 http://10.128.126.204/Mod_Network_Settings.xml). L'utilisation du module Onboard Administrator pour exécuter la commande `hponcfg` est basée sur une connexion unique à l'iLO sélectionné, au lieu de configurer le script RIBCL avec le nom d'utilisateur/mot de passe par défaut unique de l'iLO. L'application du script RIBCL réinitialise les paramètres réseau iLO sur les valeurs configurées. Répétez ces étapes pour chaque iLO. Une fois que tous les iLO dans le boîtier possèdent des adresses IP statiques configurées, désactivez le paramètre EBIPA pour les serveurs.

Possibilité 5 à l'aide de la ROM BIOS de l'iLO pendant l'opération POST du serveur :

Connectez chaque serveur à un KVM. Redémarrez chaque serveur et arrêtez l'opération POST pendant l'initialisation de la ROM de l'iLO. Modifiez la configuration réseau iLO et entrez manuellement l'adresse IP, le masque de réseau et la passerelle. Réamorcez le serveur. Répétez ces étapes pour chaque iLO.

Signaux de broche du connecteur série RS232 du module Onboard Administrator

Les broches du connecteur série DB9 (port série RS232 du module Onboard Administrator) utilisées sur le port série c7000 se présentent comme suit :

Broche	Nom	Direction	Description
1	CD	Entrée	Détection de porteuse
2	RXD	Entrée	Réception de données
3	TXD	Sortie	Transmission de données
4	DTR	Sortie	Terminal de données prêt
5	GND		Prise de masse du système
6	DSR	Entrée	Poste de données prêt
7	RTS	Sortie	Demande pour émettre
8	CTS	Entrée	Prêt à émettre
9	RI	Entrée	Indicateur d'appel

Utilisation de la connexion du port du service

Le port du service du module Onboard Administrator est le connecteur « haut » de la liaison du boîtier qui présente également une icône d'ordinateur portable en regard de la flèche pointant vers le haut. Lorsque les connecteurs de liaison du boîtier sont utilisés pour lier des boîtiers, le connecteur « haut » de la liaison du boîtier supérieur sera le port de service pour tous les boîtiers liés. Ce port est

une fiche 100BaseT Ethernet et peut être connecté directement à un connecteur d'ordinateur portable ou à un connecteur Ethernet PC RJ45 à l'aide d'un cordon de raccordement CAT5 standard étant donné que le câblage sur le connecteur « haut » de liaison est croisé pour permettre la connexion directe à un connecteur PC 100BaseT.

Le port de service fournit la connexion directe à chacun des modules Onboard Administrator actifs dans tous les boîtiers liés ou uniquement au module Onboard Administrator actif dans un boîtier unique s'il n'y a pas d'autres boîtiers liés. La connexion réseau est limitée au réseau des boîtiers et ne peut pas être utilisée pour accéder à tout périphérique à l'extérieur du réseau de supervision de boîtiers interne. Elle peut être utilisée pour accéder directement au module Onboard Administrator actif à l'adresse IP de service actif, qui s'affiche sur l'écran Enclosure Info (Info du boîtier) dans le module Insight Display du boîtier.

L'ordinateur portable ou le PC connecté au port du service du boîtier doit avoir DHCP activé pour sa connexion réseau et obtient une adresse IP comportant des zéros dans la plage 169.254.x.y après expiration du délai DHCP si l'ordinateur portable ou le PC utilise un système d'exploitation Windows. Si l'ordinateur portable ou le PC utilise Linux, vous devrez peut-être définir manuellement le port réseau sur 169.254.2.1 avec un masque de réseau de 255.255.0.0.

Pour accéder à une **interface graphique de module Onboard Administrator** active : utilisez l'adresse IP de service OA active s'affichant sur l'écran Insight Display de ce boîtier comme adresse Web dans le navigateur de votre ordinateur portable ou de votre PC. Connectez-vous à l'OA avec un compte utilisateur et un mot de passe configurés.

Pour accéder à une interface CLI de module Onboard Administrator active : utilisez un programme Telnet ou SSH basé sur les paramètres d'accès réseau configurés et connectez-vous à l'adresse IP de service OA active. Connectez-vous à l'OA avec un compte utilisateur et un mot de passe configurés.

Puisque aucun des iLO de baie de périphérique configurés n'a une adresse IP dans la plage d'adresses IP comportant des zéros, vous devez ajouter manuellement un itinéraire de réseau sur l'ordinateur portable ou sur le PC si vous devez accéder à l'adresse IP iLO depuis le port de service. La syntaxe lors de l'utilisation d'une invite de commande sur un ordinateur portable ou un PC avec système d'exploitation Windows est :

route add iLO_IP_address mask 255.255.255.255 OA_service_IP_address

Après avoir ajouté l'itinéraire vers un iLO à l'ordinateur portable ou au PC, l'iLO est accessible depuis l'interface utilisateur OA ou directement à l'aide de SSH.

Le module Onboard Administrator actif ne prend pas en charge le routage depuis le port de service vers un processeur de supervision de module d'interconnexion. Toutefois si le module d'interconnexion prend en charge la connexion série à l'OA, la commande « connect interconnect » de l'interface CLI de l'OA peut être utilisée pour se connecter à un module d'interconnexion.

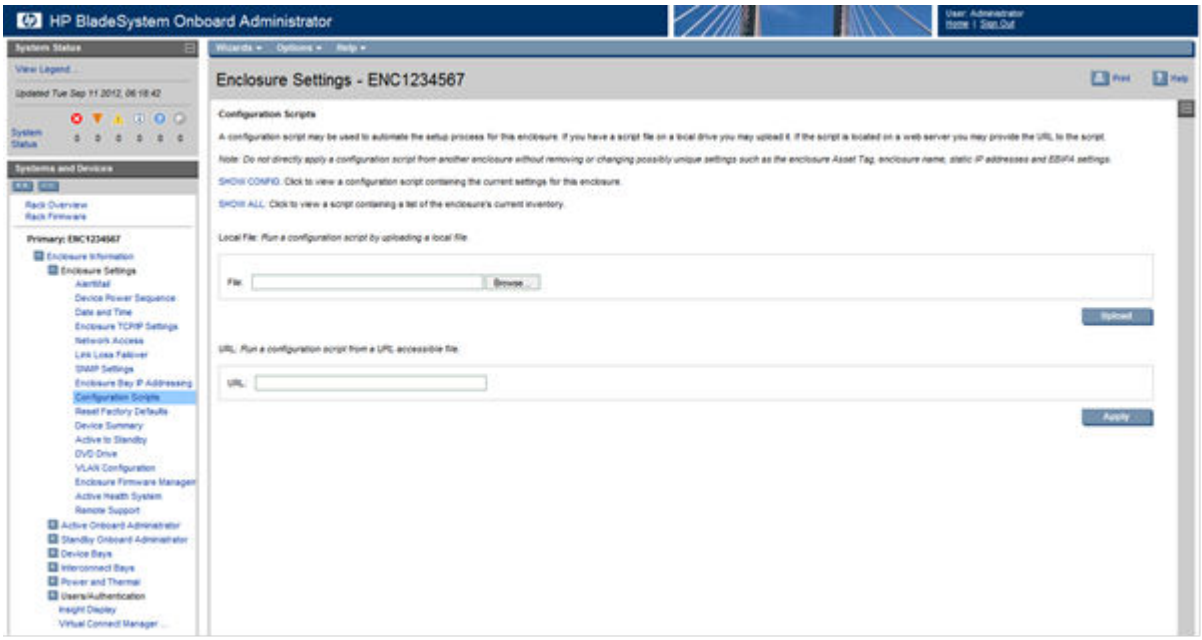
La connexion du port du service est fournie uniquement comme une connexion Ethernet temporaire au réseau privé de boîtier afin d'empêcher toute déconnexion du port de supervision du réseau de supervision externe pour l'accès au module Onboard Administrator pendant un événement de maintenance.

Utilisation de scripts de configuration

Scripts de configuration

Utilisez des scripts de configuration pour gérer des paramètres et informations de configuration, en particulier lors de la configuration de plusieurs boîtiers et modules Onboard Administrator. Cela peut éliminer la nécessité de configurer manuellement chaque boîtier. Vous pouvez créer des scripts de configuration et les utiliser dans le module Onboard Administrator via le navigateur ou la ligne de

commande, en les exécutant de la même manière qu'un script d'interpréteur de commandes dans Linux ou UNIX.



Configuration actuelle

Pour télécharger une configuration actuelle pour le boîtier :

1. Cliquez sur le lien **SHOW CONFIG** (Afficher la configuration). La configuration s'ouvre dans une nouvelle fenêtre de navigateur.
2. Pour enregistrer la configuration en tant que fichier texte, choisissez une des options suivantes :
   - Si vous utilisez Microsoft Internet Explorer, sélectionnez **Save As** (Enregistrer sous).
   - Si vous utilisez Mozilla Firefox, sélectionnez **Save Page As** (Enregistrer la page sous).
   - Si vous utilisez Google Chrome, sélectionnez **Save Link As** (Enregistrer la link sous).

Vous pouvez également sélectionner un fichier local ou une URL pour le script de configuration.

- **Fichier local** : vous pouvez rechercher le fichier de configuration ou vous pouvez entrer son chemin d'accès dans la zone de texte. Le nombre maximum de caractères dans le chemin du fichier ne peut pas dépasser 256. Après avoir saisi le chemin du fichier de configuration, cliquez sur **Upload** (Charger).
- **URL** : si le fichier de configuration est stocké sur un serveur Web, saisissez un chemin de type HTTP:// pour celui-ci. Le nombre maximum de caractères dans le chemin du fichier ne peut pas dépasser 256. Entrez l'URL, puis cliquez sur **Apply** (Appliquer).

Pour des raisons de sécurité, la configuration actuelle récupérée ne contient pas de mot de passe utilisateur. Vous pouvez modifier manuellement le script pour ajouter les mots de passe utilisateur après le nom d'utilisateur sur les lignes ADD USER. En outre, la configuration actuelle récupérée ne contient pas de paramètres LCD (Lock Buttons [Boutons de verrouillage], Enable PIN Protection [Activer la protection PIN] et PIN Code [Code PIN]). Ces paramètres ne peuvent pas être ajoutés à partir du script de configuration.

Inventaire du boîtier actuel

Pour afficher un script de l'inventaire du boîtier actuel, cliquez sur le lien **Show All** (Tout afficher). L'inventaire du boîtier actuel s'ouvre dans une nouvelle fenêtre de navigateur. Pour enregistrer l'inventaire en tant que fichier texte, choisissez une des options suivantes :

- Si vous utilisez Microsoft Internet Explorer, sélectionnez **Save As** (Enregistrer sous).
- Si vous utilisez Mozilla Firefox, sélectionnez **Save Page As** (Enregistrer la page sous).
- Si vous utilisez Google Chrome, sélectionnez **Save Page As** (Enregistrer la page sous).

Le fichier texte téléchargé fournit les mêmes informations qu'une commande CLI `SHOW ALL` (Tout afficher). Le fichier texte affiche également la configuration actuelle du boîtier.

REMARQUE : Le chargement des informations d'annuaire du boîtier dans la nouvelle fenêtre de navigation peut durer quelques minutes. Vous devez patienter jusqu'à ce que la commande `Variable list` (Liste des variables) apparaisse.

Prise en charge USB

Ce champ s'affiche lorsqu'une clé USB est détectée sur le port USB du module Onboard Administrator actif et que des fichiers de configuration sont présents. Pour télécharger un fichier de configuration, sélectionnez un fichier dans le menu, puis cliquez sur Apply (Appliquer). La taille maximale de fichier prise en charge pour les clés USB formatées avec FAT32 est de 4 Go. Pour les images SPP supérieures à 4 Go, utilisez une clé USB de format ext2.

Pour enregistrer le fichier de configuration actuel du module Onboard Administrator sur la clé USB, entrez un chemin d'accès de fichier simple, soit un chemin d'accès relatif selon le format `chemin/fichier`, soit un chemin commençant par un point (.), tel que `./chemin/fichier`, soit un chemin d'accès absolu commençant par une barre oblique (/), selon le format `/chemin/fichier`. N'entrez pas d'URL. N'incluez pas d'espaces dans le nom de fichier. Cliquez sur **Apply** (Appliquer).

Réinitialisation des valeurs usine par défaut

REMARQUE : Si le boîtier est en mode VC, vous devez effacer le mode avant de réinitialiser les valeurs usine par défaut.

REMARQUE : Avant de réinitialiser les valeurs par défaut d'usine, enregistrez votre configuration. Cliquez sur **SHOW CONFIG** pour télécharger un script contenant la configuration actuelle. Vous pouvez utiliser ce script plus tard pour restaurer les paramètres qui sont perdus après une réinitialisation d'usine.

REMARQUE : Après une réinitialisation usine, les paramètres de réseau IPv6 du boîtier (IPv6, SLAAC et DHCPv6) sont activés par défaut.

Lorsque vous réinitialisez le boîtier sur les valeurs usine par défaut, tous les paramètres du boîtier sont réinitialisés, excepté le mot de passe Administrateur intégré. Tous les paramètres AlertMail, Réseau et Protocole réseau, SNMP et Gestion de l'alimentation sont réinitialisés.

Pour réinitialiser la valeur par défaut de tous les paramètres de boîtier, y compris le mot de passe administrateur, utilisez la commande `SET FACTORY RESTORE_FACTORY_PASSWORD` de l'interface CLI de Onboard Administrator.

Pour réinitialiser le boîtier, cliquez sur **Reset Factory Defaults** (Réinitialiser les valeurs usine par défaut). Un écran de confirmation s'affiche. Pour confirmer la réinitialisation du boîtier, cliquez sur **OK**. Pour quitter sans réinitialiser le boîtier avec les paramètres par défaut, cliquez sur **Cancel** (Annuler).

REMARQUE : Cette fonction est désactivée en mode FIPS ON/DEBUG.

Pour télécharger une configuration actuelle pour le boîtier :

1. Cliquez sur le lien **SHOW CONFIG** (Afficher la configuration). La configuration s'ouvre dans une nouvelle fenêtre de navigateur.
2. Pour enregistrer la configuration en tant que fichier texte, choisissez une des options suivantes :
   - Si vous utilisez Microsoft Internet Explorer, sélectionnez **Save As** (Enregistrer sous).
   - Si vous utilisez Mozilla Firefox, sélectionnez **Save Page As** (Enregistrer la page sous).
   - Si vous utilisez Google Chrome, sélectionnez **Save Link As** (Enregistrer la link sous).

Pour des raisons de sécurité, la configuration actuelle récupérée ne contient pas de mot de passe utilisateur. Vous pouvez modifier manuellement le script pour ajouter les mots de passe utilisateur après le nom d'utilisateur sur les lignes ADD USER. En outre, la configuration actuelle récupérée ne contient pas de paramètres LCD (Lock Buttons [Boutons de verrouillage], Enable PIN Protection [Activer la protection PIN] et PIN Code [Code PIN]). Ces paramètres ne peuvent pas être ajoutés à partir du script de configuration.

L'effacement du mode VC supprime tous les paramètres VC du boîtier. Mettez hors tension tous les serveurs configurés VC avant d'effacer le mode VC. Si les serveurs ne sont pas mis hors tension, ils risquent de conserver leurs paramètres VC jusqu'à leur redémarrage. Vous devez effacer le mode VC avant de passer au mode FIPS OFF/ON/DEBUG.

Pour effacer le mode VC :

1. Cliquez sur **Clear VC Mode** (Effacer mode VC). Un écran de confirmation s'affiche, indiquant un message signifiant `Tous les serveurs doivent être mis hors tension et non configurés par Virtual Connect avant l'effacement du mode VC. Souhaitez-vous vraiment effacer le mode VC ?`
2. Cliquez sur **OK**.

10 Prise en charge de lame de serveur HP Integrity i2

Prise en charge mise à jour pour lames de serveur HP Integrity BL860c i2, BL870c i2 et BL890c i2

Les lames de serveur HP Integrity i2 incluent des ensembles matériels Blade Link qui conjuguent plusieurs lames de serveur BL860c i2 pour créer des serveurs double lame à quatre prises et des serveurs quadruple lame à huit prises.

La version 3.00 ou ultérieure du microprogramme Onboard Administrator est requise pour prendre en charge ces lames de serveur.

L'arborescence de l'interface graphique utilisateur Onboard Administrator GUI et la vue graphique ont été mises à jour pour prendre en charge les lames de serveur HP Integrity i2. Les écrans Port Mapping (Mappage de ports), Firmware (Microprogramme) et Partner Blade (Lame partenaire) ont également été mis à jour.

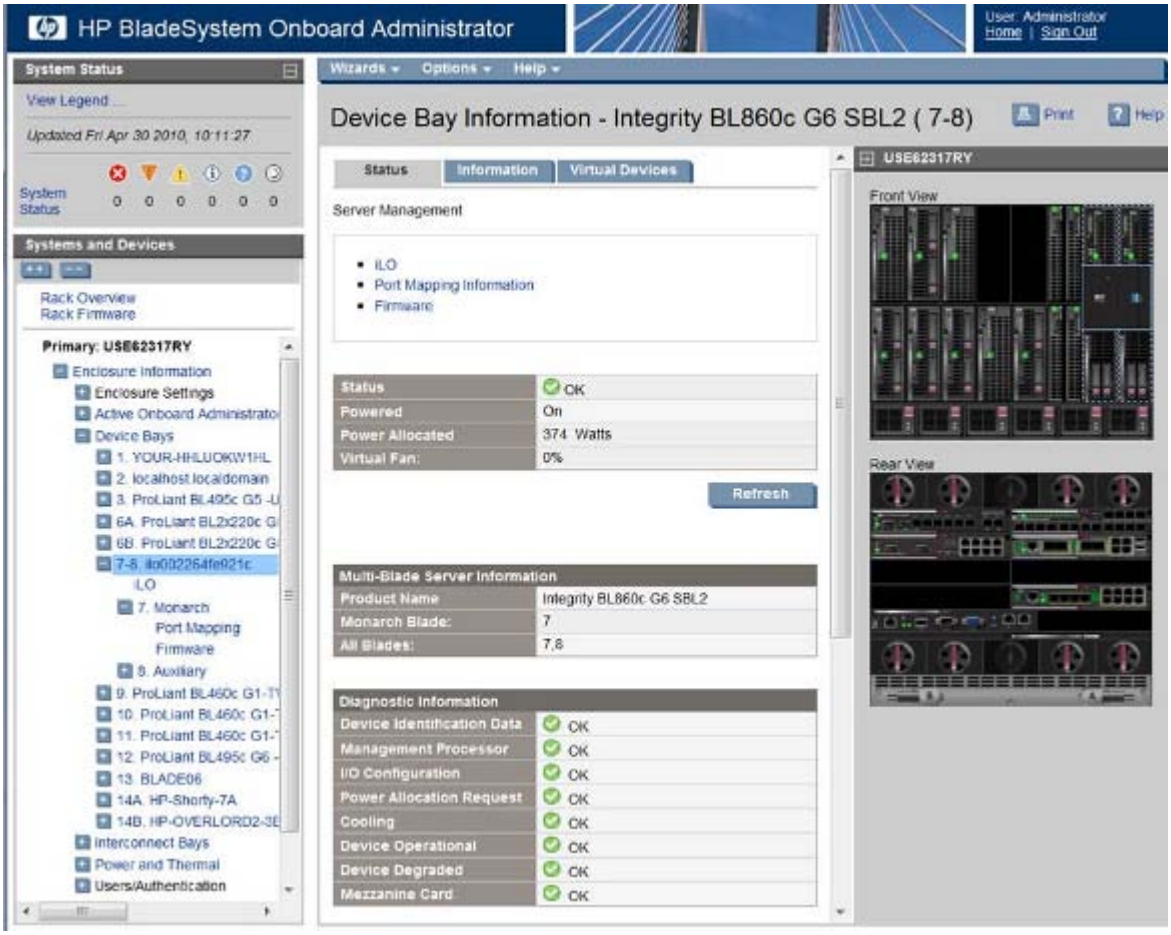
Modification de vue d'arborescence et de vue graphique pour lames de serveur HP Integrity i2

Toutes les lames de serveur HP Integrity i2 comportent un lien Blade Link. L'entrée de vue d'arborescence principale pour une lame de serveur conjointe indique la plage de baies contenant toutes les lames de serveur individuelles qui sont conjointes.

La sélection de l'entrée de vue d'arborescence principale de la lame de serveur conjointe met en évidence le lien Blade Link dans la vue graphique avec un cadre bleu plein, et chacune des lames de serveur conjointes et lames partenaires associées sont mises en évidence individuellement avec des cadres bleus en pointillés. Le titre Device Bay Information (Informations de baie de périphérique) inclut la taille du lien Blade Link et la plage des baies dans le serveur conjoint.

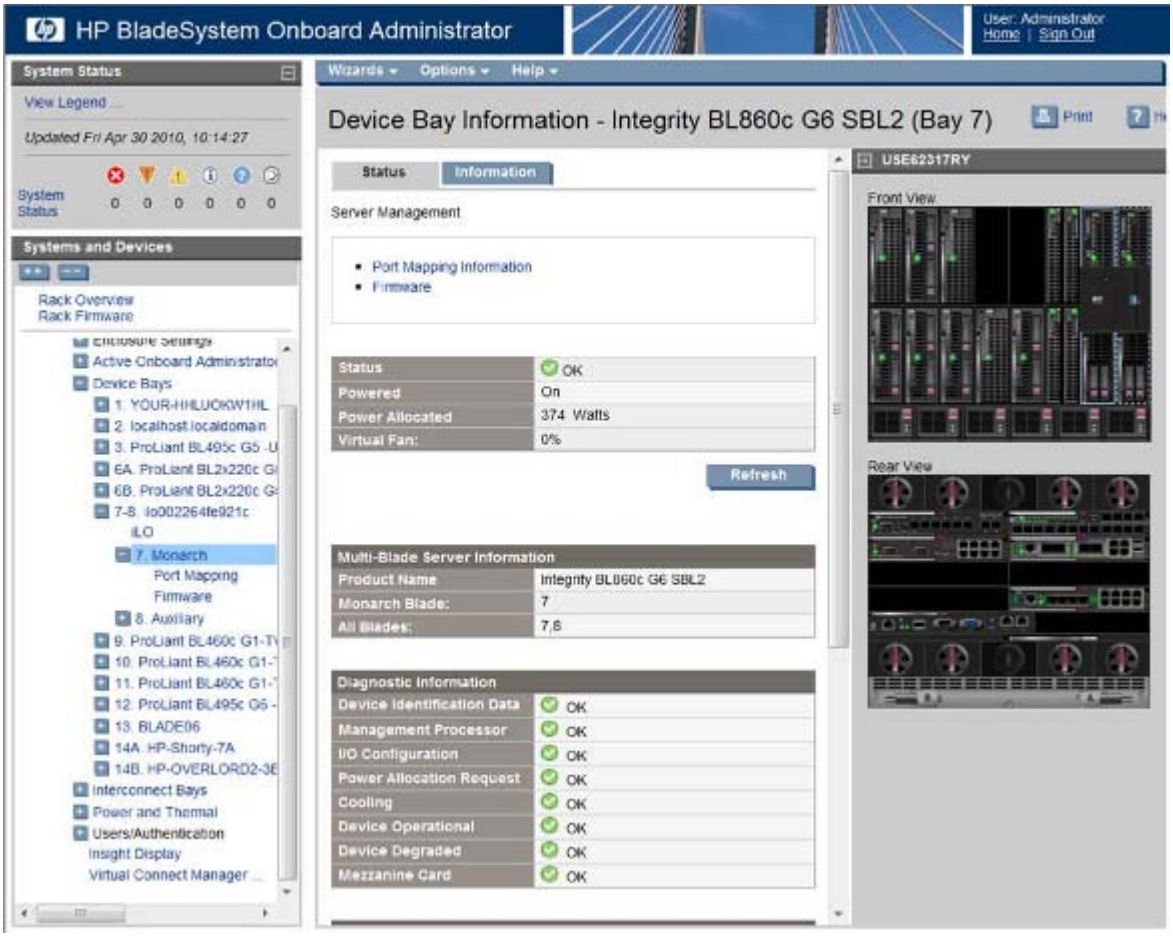
L'onglet Virtual Device (Périphérique virtuel) de l'écran Device Bay Information est uniquement disponible sur l'entrée principale de la vue d'arborescence pour la lame de serveur conjointe entière.

L'entrée iLO dans la vue d'arborescence est uniquement sous l'entrée principale de la lame de serveur conjointe entière.



Un nouvel élément est ajouté à la vue d'arborescence sous le système iLO de la lame de serveur conjointe intitulé Monarch ou Auxiliary sur la base du rôle de cette lame de serveur dans le serveur conjoint.

La sélection de Monarch ou Auxiliary permet de naviguer vers la page Device Bay Information pour cette lame spécifique. La lame sélectionnée est dotée d'une mise en évidence en bleu plein dans la vue graphique, et les autres lames de serveur conjointes et toutes les lames partenaires associées comportent une mise en évidence bleu en pointillés. Le tableau Multi-Blade Server Information indique le nom du produit et la baie Monarch, et répertorie également toutes les lames de serveur du serveur conjoint.



Modification de mappage de ports pour lames de serveur HP Integrity i2

Le mappage de ports pour les lames de serveur conjointes est affiché sur chaque lame de serveur individuelle sélectionnée dans la vue d'arborescence sous le rôle Monarch ou Auxiliary de cette lame de serveur.

Modifications de lames partenaires pour lames de serveur HP Integrity i2

Une lame de serveur conjointe HP Integrity i2 peut comporter au maximum trois lames partenaires. Pour plus d'informations, consultez le document *HP Integrity i2 Server Blade Installation Guide* (Manuel d'installation de la lame de serveur HP Integrity i2) approprié dans HP Enterprise Information Library. (Sous **Products and Solutions** (Produits et solutions), sélectionnez **HP BladeSystem**. Sous **HP BladeSystem**, sélectionnez **Integrity Server Blades** (Lames de serveur Integrity.)

11 Résolution des problèmes

Messages d'erreur du module Onboard Administrator

- Erreurs de réponse Soap : Il s'agit des erreurs générales rapportées par le service gSoap pour les erreurs de validation, les erreurs de périphérique, etc. Ces erreurs sont classées en deux catégories :
  - Erreurs de demande utilisateur
  - Erreurs Onboard Administrator
- Erreurs d'interface Soap : ces erreurs signalent des problèmes internes avec le service gSoap.
- Erreurs d'application CGI : ces erreurs sont rapportées par des processus CGI individuels. Chacune d'elles émet son propre groupe d'erreurs :
  - Erreurs de téléchargement de fichier
  - Erreurs de capture d'écran Insight Display

Erreurs Onboard Administrator

1 The submitted user already exists. (L'utilisateur soumis existe déjà.)

2 The submitted user name is not valid. (Le nom de l'utilisateur soumis n'est pas valide.)

3 The maximum number of users already exists. (Le nombre maximum d'utilisateurs existe déjà.)

5 The requested user does not exist. (L'utilisateur demandé n'existe pas.)

6 The submitted group already exists. (Le groupe soumis existe déjà.)

7 Invalid privilege level. (Niveau de privilège non valide.)

8 Insufficient privileges for the requested operation. (Privilèges insuffisants pour l'opération demandée.)

10 The submitted user was already enabled. (L'utilisateur soumis est déjà activé.)

11 The submitted user was already disabled. (L'utilisateur soumis est déjà désactivé.)

12 The submitted user already has administrator rights. (L'utilisateur soumis dispose déjà de droits d'administrateur.)

13 The submitted user is not an administrator. (L'utilisateur soumis n'est pas un administrateur.)

14 An error occurred while creating a group entry. (Une erreur s'est produite lors de la création d'une entrée de groupe.)

16 Unable to perform the operation. (Impossible d'effectuer l'opération.) Retry the operation or restart OA. (Recommencez l'opération ou redémarrez OA) (System Error 16) (Erreur système 16)

17 Unable to perform the operation. (Impossible d'effectuer l'opération.) Retry the operation or restart OA. (Recommencez l'opération ou redémarrez OA) (System Error 17) (Erreur système 17)

18 Unable to perform the operation. (Impossible d'effectuer l'opération.) Retry the operation or restart OA. (Recommencez l'opération ou redémarrez OA) (System Error 18) (Erreur système 18)

19 The submitted bay is already assigned. (La baie soumise est déjà attribuée.)

20 The submitted bay is not assigned. (La baie soumise n'est pas attribuée.)

22 The submitted value is already in use. (La valeur soumise est déjà utilisée.)

23 The first character in the submitted value is not valid. (Le premier caractère de la valeur soumise n'est pas valide.)

24 The submitted value contains an invalid character. (La valeur soumise contient un caractère non valide.)

25 The submitted value is too short. (La valeur soumise est trop courte.)

26 The submitted value is too long. (La valeur soumise est trop longue.)

27 The submitted trap receiver already exists. (Le récepteur d'interruptions soumis existe déjà.)

28 The maximum number of trap receivers already exists. (Le nombre maximum de récepteurs d'interruptions existe déjà.)

29 The maximum number of IP managers already exists. (Le nombre maximum de gestionnaires IP existe déjà.)

30 The IP Manager already exists. (Le gestionnaire IP existe déjà.)

31 The submitted bay number is out of range. (Le numéro de baie soumis est hors plage.)

32 The submitted IP address is not valid. (L'adresse IP soumise n'est pas valide.)

33 The submitted value is null. (La valeur soumise est nulle.)

34 An error occurred while generating an event. (Une erreur s'est produite lors de la génération d'un événement.)

35 An error occurred opening the enclosure system log. (Une erreur s'est produite lors de l'ouverture du journal système du boîtier.)

36 The submitted date and/or time value was not formatted correctly. (Le format de la valeur de date et/ou d'heure soumise n'est pas correct.)

37 An error occurred while opening the Onboard Administrator's system log. (Une erreur s'est produite lors de l'ouverture du journal système du module Onboard Administrator.)

38 The NMI Dump failed for the submitted blade. (Échec du vidage NMI pour la lame soumise.)

39 Setting the UID for the submitted blade failed. (Échec de la définition de l'UID pour la lame soumise.)

40 Setting the environment variable for the submitted blade failed. (Échec de la définition de la variable d'environnement pour la lame soumise.)

41 Setting the boot order for the submitted blade failed. (Échec de l'ordre de démarrage pour la lame soumise.)

42 Setting the power control for the submitted blade failed. (Échec du contrôle d'alimentation pour la lame soumise.)

43 Setting the max power for the submitted bladed failed. (Échec de la définition de la puissance maximale pour la lame soumise.)

44 Shutting down the submitted blade failed. (Échec de la mise hors tension de la lame soumise.)

45 Clearing the submitted blade failed. (Échec de l'effacement de la lame soumise.)

46 Getting blade information for the submitted blade failed. (Échec de l'obtention d'informations pour la lame soumise.)

47 Getting blade status for the submitted blade failed. (Échec de l'obtention de l'état pour la lame soumise.)

48 Getting sensor information for the submitted sensor failed. (Échec de l'obtention des informations de capteur pour la lame soumise.)

49 Setting the submitted rack name failed. (Échec de la définition du nom du rack soumis.)

50 Getting power supply information for the submitted power supply failed. (Échec de l'obtention des informations sur l'alimentation pour l'alimentation soumise.)

51 Getting power supply status for the submitted power supply failed. (Échec de l'obtention de l'état de l'alimentation pour l'alimentation soumise.)

52 Getting power supply measurements for the submitted power supply failed. (Échec de l'obtention des mesures de l'alimentation pour l'alimentation soumise.)

53 Setting the Onboard Administrator's UID state failed. (Échec de la définition de l'état de l'UID du module Onboard Administrator.)

54 Getting the Onboard Administrator's status failed. (Échec de l'obtention de l'état du module Onboard Administrator.)

55 Getting the Onboard Administrator's information failed. (Échec de l'obtention des informations du module Onboard Administrator.)

56 Getting fan information for the submitted fan failed. (Échec de l'obtention des informations de ventilateur pour le ventilateur soumis.)

57 Rebooting the enclosure failed. (Échec du redémarrage du boîtier.)

58 Shutting down the enclosure failed. (Échec de la mise hors tension du boîtier.)

59 Getting the enclosure information failed. (Échec de l'obtention des informations du boîtier.)

60 Getting the enclosure names failed. (Échec de l'obtention des noms de boîtier.)

61 Getting the enclosure status failed. (Échec de l'obtention de l'état du boîtier.)

62 Setting the enclosure name failed. (Échec de la définition du nom du boîtier.)

63 Setting the enclosure asset tag failed. (Échec de la définition de l'étiquette du boîtier.)

64 Setting the enclosure time zone failed. (Échec de la définition du fuseau horaire du boîtier.)

65 Setting the enclosure UID failed. (Échec de la définition de l'UID du boîtier.)

66 Setting the UID for the submitted interconnect failed. (Échec de la définition de l'UID pour l'interconnexion soumise.)

67 Resetting the submitted interconnect failed. (Échec de la réinitialisation de l'interconnexion soumise.)

68 Getting interconnect information for the submitted interconnect failed. (Échec de l'obtention des informations de l'interconnexion pour l'interconnexion soumise.)

69 Getting interconnect status for the submitted interconnect failed. (Échec de l'obtention de l'état de l'interconnexion pour l'interconnexion soumise.)

70 An error occurred while accessing the connected user for the requested blade. (Une erreur s'est produite lors de l'accès de l'utilisateur connecté pour la lame demandée.)

71 An error occurred while reading the lockfile for the submitted blade. (Une erreur s'est produite lors de la lecture du fichier de verrouillage pour la lame soumise.)

72 The submitted E-mail address is not valid. (L'adresse électronique soumise n'est pas valide.)

73 Libem is not able to talk to iLO. (Libem ne peut pas parler à iLO.)

74 Downloading the submitted file failed. (Échec du téléchargement du fichier soumis.)

75 The certificate could not be verified. (Impossible de vérifier le certificat.)

76 Could not save the authorization keys. (Impossible d'enregistrer les clés d'autorisation.)

77 The SSH key size is not correct. (La taille de clé SSH n'est pas correcte.)

78 Could not ping the requested url. (Impossible de lancer une requête ping sur l'URL demandée.)

79 Could not generate the CSR. (Impossible de générer le CSR.)

80 Could not generate the SSO. (Impossible de générer le SSO.)

81 Could not read the fingerprint. (Impossible de lire l'empreinte.)

82 Could not get SSH key. (Impossible d'obtenir la clé SSH.)

83 The field is already enabled. (Le champ est déjà activé.)

84 The field is already disabled. (Le champ est déjà désactivé.)

85 The system is already in DHCP mode. (Le système est déjà en mode DHCP.)

86 The system is currently in static IP mode. (Le système est actuellement en mode IP statique.)

87 Could not clear the system log. (Impossible d'effacer le journal système.)

88 Could not restore the factory settings. (Impossible de restaurer les paramètres usine.)

89 Could not read the configuration file. (Impossible de lire le fichier de configuration.)

90 Could not write to the configuration file. (Impossible d'écrire dans le fichier de configuration.)

92 The submitted url is not valid. (L'URL soumise n'est pas valide.)

93 Could not update the firmware with the submitted image file. (Impossible de mettre à jour le microprogramme avec le fichier d'image soumis.)

94 Unable to acquire the rack topology. (Impossible d'acquérir la topologie du rack.)

95 Invalid domain. (Domaine non valide.)

97 Connecting to the blade's iLO failed. (Échec de la connexion au iLO de la lame.)

98 Sending the RIBCL command to the requested blade failed. (Échec de l'envoi de la commande RIBCL à la lame demandée.)

99 Could not find the requested element in the RIBCL response. (Impossible de trouver l'élément demandé dans la réponse RIBCL.)

100 Could not find the requested attribute in the RIBCL response. (Impossible de trouver l'attribut demandé dans la réponse RIBCL.)

101 Could not find the starting boundary in the RIBCL response. (Impossible de trouver la limite de départ dans la réponse RIBCL.)

102 Could not find the ending boundary in the RIBCL response. (Impossible de trouver la limite de fin dans la réponse RIBCL.)

103 Could not determine the IP address of the management processor for the requested blade. (Impossible de déterminer l'adresse IP du processeur de supervision pour la lame demandée.)

104 Could not locate a Primary NTP server. (Impossible de trouver un serveur NTP principal.)

105 You must set at least one (1) trusted host before enabling trusted hosts. (Vous devez définir au moins un (1) hôte certifié avant d'activer des hôtes certifiés.)

107 Could not create the RIBCL request. (Impossible de créer la requête RIBCL.)

108 This error message should be taken from the soap errorText (varies). (Ce message d'erreur doit être pris dans le processus SOAP errorText (variations possibles).)

118 The management processor auto-login feature is not supported. (La fonction de connexion automatique du processeur de supervision n'est pas prise en charge.)

119 The maximum number of EBIPA DNS servers has already been reached. (Le nombre maximum de serveurs DNS EBIPA est déjà atteint.)

120 The starting IP address and Net Mask must be set before enabling EBIPA. (L'adresse IP de début et le masque de réseau doivent être définis avant d'activer EBIPA.)

121 The LDAP group does not exist. (Le groupe LDAP n'existe pas.)

122 The LDAP group already exists. (Le groupe LDAP existe déjà.)

123 The maximum number of LDAP groups has already been reached. (Le nombre maximum de groupes LDAP est déjà atteint.)

125 Error getting Insight Display information. (Erreur lors de l'obtention des informations sur Insight Display.)

126 Error getting Insight Display status. (Erreur lors de l'obtention de l'état de Insight Display.)

127 Error reading the certificate. (Erreur lors de la lecture du certificat.)

128 Error setting the time zone. (Erreur lors de la définition du fuseau horaire.)

129 Error installing the certificate. (Erreur lors de l'installation du certificat.)

130 Exceeded the maximum number of SSO certificates. (Nombre maximum de certificats CA dépassé.)

131 The X509 Certificate is not formatted correctly. (Format du certificat X509 incorrect.)

132 HP SIM station already in trusted list. (Le poste HP SIM est déjà dans une liste certifiée.)

133 HP SIM station name not found. (Nom du poste HP SIM introuvable.)

134 HP SIM SSO API received a bad parameter. (L'API SSO de HP SIM a reçu un paramètre incorrect.)

135 The maximum number of HP SIM XE stations already configured. (Le nombre maximum de postes XE HP SIM est déjà configuré.)

136 The maximum number of EBIPA interconnects DNS servers has been reached. (Le nombre maximum de serveurs DNS d'interconnexions EBIPA a été atteint.)

137 The session could not be created. (Impossible de créer la session.)

138 The session could not be deleted. (Impossible de supprimer la session.)

139 Not a valid request while running in standby mode. (Demande non valide pendant une exécution en mode Standby.)

140 Not a valid request while transitioning to active mode. (Demande non valide pendant un passage en mode actif.)

141 Not a valid request while running in active mode. (Demande non valide pendant une exécution en mode actif.)

142 The maximum number of LDAP certificates already exist. (Le nombre maximum de certificats LDAP existe déjà.)

143 Could not remove LDAP certificate. (Impossible de supprimer le certificat LDAP.)

144 You must configure the directory server and at least one search context before enabling LDAP. (Vous devez configurer le serveur d'annuaires et au moins un contexte de recherche avant d'activer LDAP.)

145 Could not set the LDAP group description. (Impossible de définir la description du groupe LDAP.)

146 An error occurred while communicating with the other Onboard Administrator. (Une erreur s'est produite lors de la communication avec l'autre Onboard Administrator.)

147 Unable to perform the operation. (Impossible d'effectuer l'opération.) Retry the operation or restart OA. (Recommencez l'opération ou redémarrez OA) (System Error 147) (Erreur système 147)

148 The other Onboard Administrator is not present. (L'autre Onboard Administrator n'est pas présent.)

149 No redundant Onboard Administrator found. (Aucun Onboard Administrator redondant n'a été trouvé.) Cannot failover. (Basculement impossible.)

150 The user could not be authenticated. (Impossible d'authentifier l'utilisateur.)

151 Invalid parameter for setting blade one time boot. (Paramètre non valide pour définir le démarrage unique de la lame.)

152 Invalid parameter for setting the blade boot priority. (Paramètre non valide pour définir la priorité du démarrage de la lame.)

153 A blade boot device can only be listed once. (Un périphérique de démarrage de lame ne peut être répertorié qu'une seule fois.)

154 NTP Poll time must be between 60 and 86400 seconds. (La durée du sondage NTP doit être comprise entre 60 et 86400 secondes.)

155 Could not create new file. (Impossible de créer le fichier.)

156 Could not write the file to the disk. (Impossible d'écrire le fichier sur le disque.)

157 The submitted image is too big. (L'image soumise est trop grande.)

158 The submitted image is not a BMP image. (L'image soumise n'est pas une image BMP.)

159 The submitted image does not have the appropriate dimensions. (Les dimensions de l'image soumise ne sont pas appropriées.)

160 Non-standard BMP images are not supported. (Les images BMP non standard ne sont pas prises en charge.)

161 The specified item was not found. (Élément spécifié introuvable.)

162 The protocol specified in the URL is not supported. (Le protocole spécifié dans l'URL n'est pas pris en charge.)

163 The upload to the specified URL failed. (Échec du téléchargement vers l'URL spécifiée.)

164 The Onboard Administrator did not fail over. (Échec du basculement du module Onboard Administrator.)

165 The blade is in a powered off state. (La lame est en état non activé.)

167 The IP manager does not exist. (Le gestionnaire IP n'existe pas.)

168 There is no SSH key installed. (Aucune clé SSH n'est installée.)

169 There was a problem running the configuration script. (Un problème est survenu lors de l'exécution du script de configuration.)

170 Missing credentials. (Informations de connexion manquantes.)

171 Caught the SIGSEGV signal. (Signal SIGSEGV détecté.)

173 No trap receivers were specified. (Aucun récepteur d'interruptions n'a été spécifié.)

174 There are no SSH keys installed. (Aucune clé SSH n'est installée.)

175 There was an error attempting to clear the SSH keys. (Une erreur s'est produite lors d'une tentative d'effacement des clés SSH.)

176 The IP address is already listed. (L'adresse IP est déjà répertoriée.)

177 There was an error getting the SSO trust mode. (Une erreur s'est produite lors d'obtention du mode de confiance SSO.)

178 The submitted SSO trust mode is invalid. (Le mode de confiance SSO soumis n'est pas valide.)

179 The certificate cannot be removed because it does not exist. (Le certificat ne peut pas être supprimé car il n'existe pas.)

180 The interconnect tray is not present. (Le tiroir d'interconnexion n'est pas présent.)

181 The blade is not present. (La lame n'est pas présente.)

182 Users cannot remove or disable themselves. (Les utilisateurs ne peuvent pas se supprimer ou se désactiver eux-mêmes.)

183 Invalid time zone. (Fuseau horaire non valide).

184 Error setting CLP strings. (Erreur de définition de chaînes CLP).

185 Error getting CLP status. (Erreur d'obtention d'état CLP).

186 Error setting ISMIC info block. (Erreur de définition de bloc d'infos ISMIC).

187 Error reading ISMIC info block. (Erreur de lecture de bloc d'infos ISMIC).

188 Error clearing blade signature. (Erreur d'effacement de signature de lame).

189 Error setting blade signature. (Erreur de définition de signature de lame).

190 Request is valid only for server blades. (Demande uniquement valide pour lames de serveur).

191 Request is valid only for ProLiant server blades. (Demande uniquement valide pour lames de serveur ProLiant).

192 The string entered is not a valid netmask. (La chaîne entrée n'est pas un masque réseau valide.)

193 The string entered is not a valid gateway. (La chaîne entrée n'est pas une passerelle valide.)

194 The string entered for DNS server 1 is not valid. (La chaîne entrée pour le serveur DNS 1 n'est pas valide.)

195 The string entered for DNS server 2 is not valid. (La chaîne entrée pour le serveur DNS 2 n'est pas valide.)

196 Error trying to remove a nonexistent SSO name. (Erreur de tentative de suppression d'un nom SSO inexistant).

197 Error trying to add an SSO name. (Erreur de tentative d'ajout un nom SSO).

198 Invalid SNMP trap community. (Communauté d'interruptions SNMP non valide).

201 Could not open the event pipe for reading. (Impossible d'ouvrir le canal d'événements pour lecture.)

202 Did not read the proper size for events. (Taille appropriée non lue pour les événements.)

203 Event length mismatch. (Discordance de longueur d'événement.)

204 The event listener was terminated. (L'écouteur d'événements a été terminé.)

211 Error obtaining blade power reduction status. (Erreur d'obtention d'état de réduction d'alimentation de lame).

212 Update the other OA firmware to enable this feature. (Mettez à jour le microprogramme d'autres modules OA pour activer cette fonction.)

213 Dates before 14 June 2006 are not valid. (Les dates avant le 14 juin 2006 ne sont pas valables).

214 The certificate exceeds the maximum valid size. (Le certificat dépasse la taille maximale valide.)

215 E-Fuse cannot be reset. (Impossible de réinitialiser la fonction E-Fuse.)

216 Firmware update in progress. (Mise à jour du microprogramme en cours) Login is disabled. (connexion impossible.)

217 An error occurred while setting the enclosure PDU type. (Une erreur s'est produite lors de la définition du type d'unité PDU du boîtier.)

218 An error occurred while setting the enclosure part number. (Une erreur s'est produite lors de la définition du numéro de référence du boîtier.)

219 An error occurred while setting the enclosure serial number. (Une erreur s'est produite lors de la définition du numéro de série du boîtier.)

220 Cannot set time when NTP is enabled. (Impossible de régler l'heure lorsque le protocole NTP est activé.)

221 Request is valid only for Itanium/BCS/IPF blades. (La demande est valable uniquement pour les lames Itanium/BCS/IPF.)

222 The Active and Standby Onboard Administrator are not the same hardware build. (Les modules Onboard Administrator actif et en mode Standby n'ont pas la même version de matériel.)

223 The firmware installed on an Onboard Administrator module is incompatible with FirmwareSync. (Le microprogramme installé sur un module Onboard Administrator est incompatible avec FirmwareSync.)

224 Failed to create firmware image. (Échec de création de l'image du microprogramme.)

225 The Active and Standby Onboard Administrator have the same firmware version installed. (Les modules Onboard Administrator actif et en mode Standby ont la même version de microprogramme installée.)

226 Upgrade an Onboard Administrator to firmware 2.10 or later to enable this feature. (Mettez à niveau un module Onboard Administrator au microprogramme 2.10 ou version ultérieure pour activer cette fonction.)

227 The requested user cannot be removed from iLO because it is the only remaining administrator account. (L'utilisateur demandé ne peut pas être supprimé de la carte iLO car il est le seul compte administrateur restant.)

228 The requested user cannot be added to iLO because iLO local accounts have been disabled. (L'utilisateur demandé ne peut pas être ajouté à la carte iLO car les comptes locaux iLO ont été désactivés.)

229 The requested user cannot be added to iLO because the maximum number of local accounts already exists. (L'utilisateur demandé ne peut pas être ajouté à la carte iLO car le nombre maximum de comptes locaux iLO existe déjà.)

230 One or more of the specified SNMP traps were not already configured on the Onboard Administrator and cannot be removed. (Une ou plusieurs des interruptions SNMP spécifiées n'étaient pas déjà configurées sur le module Onboard Administrator et ne peuvent pas être supprimées.)

231 Reset Factory Defaults in progress. (Restauration des paramètres d'usine en cours) Login disabled. (connexion impossible.)

232 The requested operation is not available on c3000 enclosures. (L'opération demandée n'est pas disponible sur les boîtiers c3000.)

233 This feature requires the iLO Select Pack License or iLO Advanced Pack License on the server blade when LDAP is enabled on the Onboard Administrator. (Cette fonction nécessite la licence iLO Select Pack ou iLO Advanced Pack sur la lame de serveur lorsque LDAP est activé sur le module Onboard Administrator.)

234 Invalid characters detected. (Caractères non valides détectés.)

235 HP Onboard Administrator is initializing. (Initialisation de HP Onboard Administrator en cours) Login disabled. (connexion impossible.)

236 Cannot retrieve Onboard Administrator media device array. (Impossible de récupérer le plateau de périphériques multimédia Onboard Administrator.)

237 The requested device is not ready. (Le périphérique demandé n'est pas prêt.)

238 Power off or remove the partner blade. (Mettez hors tension ou retirez la lame partenaire.)

239 The current firmware does not support this operation. (Le microprogramme actuel ne prend pas en charge cette opération.)

240 Serial number update requires newer firmware version. (La mise à jour du numéro de série nécessite une version plus récente du microprogramme.)

241 The requested device is not present or no firmware upgrade is required. (Le périphérique demandé n'est pas présent ou aucune mise à niveau du microprogramme n'est nécessaire.)

242 The operation cannot be performed on the requested device. (L'opération ne peut pas être effectuée sur le périphérique demandé.)

243 iLO license information cannot be retrieved because iLO XML Reply is disabled. (Impossible de récupérer les informations de licence iLO car la réponse XML iLO est désactivée.)

244 SSH is disabled on this blade. (SSH est désactivé sur cette lame.)

245 Disconnect the virtual media applet. (Déconnectez l'applet de support virtuel.)

246 Invalid SNMP Write Community string. (Chaîne de communauté d'écriture SNMP non valide).

247 Invalid SNMP Read Community string. (Chaîne de communauté de lecture SNMP non valide).

248 Invalid port number. The LDAP server SSL port can be any number between 1 and 65535. (Numéro de port non valide, le port SSL du serveur LDAP doit être un chiffre compris entre 1 et 65535.)

249 Feb 29 was specified but the year is not a leap year. (29 février a été spécifié, mais l'année n'est pas une année bissextile.)

250 The CA certificate is invalid. (Le certificat CA n'est pas valide.)

251 Exceeded the maximum number of CA certificates. (Nombre maximum de certificats CA dépassé.)

252 No CA certificates are imported. (Aucun certificat CA importé.)

253 This CA certificate is already imported. (Ce certificat CA est déjà importé.)

254 A certificate is already mapped to this user. (Un certificat est déjà mappé sur cet utilisateur.)

255 An undocumented error has occurred. (Une erreur non documentée s'est produite.) Please update your firmware to the latest firmware version if necessary. (Mettez votre microprogramme à jour avec la dernière version du microprogramme, si nécessaire.) Contact HP if the problem persists. (Si le problème persiste, contactez HP.)

256 This certificate is already mapped to another user. (Ce certificat est déjà mappé sur un autre utilisateur.)

257 The user certificate could not be verified. (Impossible de vérifier le certificat utilisateur.)

258 This operation is not permitted when two-factor authentication is enabled. (Cette opération n'est pas autorisée lorsque l'authentification à deux facteurs est activée.)

260 This operation cannot be performed when AlertMail is disabled. (Cette opération ne peut pas être effectuée lorsque AlertMail est désactivé.)

261 This operation cannot be performed when the AlertMail settings are not configured. (Cette opération ne peut pas être effectuée lorsque les paramètres AlertMail ne sont pas configurés.)

262 This operation cannot be performed when SNMP is disabled. (Cette opération ne peut pas être effectuée lorsque SNMP est désactivé.)

263 A certificate must be mapped to Administrator or LDAP must be enabled with a configured groups with administrator privilege to enable two-factor authentication. (Un certificat doit être mappé sur l'administrateur ou LDAP doit être activé avec un des groupes configurés avec des privilèges d'administrateur pour activer l'authentification à deux facteurs.)

265 A certificate is not mapped to this user account. (Aucun certificat n'est mappé sur ce compte utilisateur.)

266 Two-factor authentication is in effect. (L'authentification à deux facteurs est en vigueur.)

267 Two-factor authentication configuration was not changed. (La configuration de l'authentification à deux facteurs n'a pas été modifiée.)

268 An iLO image is already staged. (Une image iLO est déjà organisée.)

269 The file was not a proper iLO image for the blade. (Le fichier n'avait pas une image iLO correcte pour la lame.)

270 The crc32 supplied does not match the provided file. (Le crc32 fourni ne correspond pas au fichier fourni.)

271 Cannot delete the last CA with two-factor authentication enabled. (Impossible de supprimer le dernier CA avec l'authentification à deux facteurs activée.)

272 The Onboard Administrator cannot communicate with iLO. (Le module Onboard Administrator ne peut pas communiquer avec iLO.)

273 An EBIPA configuration error occurred. (Une erreur de configuration EBIPA s'est produite.)

274 Link Loss Failover intervals must be between 30 and 86400 seconds. (Les intervalles sur basculement de perte de liaison doivent être compris entre 30 et 86400 secondes.)

275 Network speed must be either 10Mbit or 100Mbit. (La vitesse du réseau doit être 10Mbit ou 100Mbit.)

276 Network duplex setting must be HALF or FULL. (Le paramètre duplex réseau doit être HALF ou FULL.)

277 The password does not conform to password rules. (Le mot de passe n'est pas conforme aux règles de mot de passe.)

278 Invalid minimum password value. (Valeur de mot de passe minimum non valide).

279 An firmware image is already staged. (Une image de microprogramme est déjà organisée.)

280 The provided file was not a proper image. (Le fichier fourni n'est pas une image correcte.)

281 Bad image CRC checksum. (Somme de contrôle CRC d'image incorrecte).

282 Remote system logging must be enabled to perform this operation. (La journalisation système à distance doit être activée pour effectuer cette opération.)

283 Invalid remote port. (Numéro de port distant non valide) The port must be a number between 1 and 65535. (Le port doit être un chiffre compris entre 1 et 65535.)

284 The remote syslog server address must be configured before enabling remote system logging. (L'adresse du serveur syslog distant doit être configurée avant d'activer la journalisation système à distance.)

285 Invalid remote server address. (Adresse du serveur distant non valide).

286 This setting is already enabled. (Ce paramètre est déjà activé.)

287 This setting is already disabled. (Ce paramètre est déjà désactivé.)

288 Enclosure IP mode was not enabled because the active Onboard Administrator does not have a static IPv4 address. (Le mode IP du boîtier n'a pas été activé car le module Onboard Administrator actif ne possède pas d'adresse IPv4 statique.)

289 This feature is not available for this Onboard Administrator. (Cette fonction n'est pas disponible pour ce module Onboard Administrator.)

290 Request to enable DHCP addressing on the active Onboard Administrator is denied because Enclosure IP Mode is enabled. (La demande d'activation d'adressage DHCP sur le module Onboard Administrator actif est refusée car le mode IP du boîtier est activé.)

291 The value provided is not proper base64. (La valeur fournie n'est pas une valeur base64 correcte.)

292 The firmware image provided is an older version than the current firmware. (L'image de microprogramme fournie correspond à une version antérieure au microprogramme actuel.) Onboard Administrator settings cannot be preserved. (Les paramètres Onboard Administrator ne peuvent pas être conservés.)

293 The file provided is not a valid Onboard Administrator firmware image. (Le fichier fourni n'est pas une image de microprogramme Onboard Administrator valide.)

294 There are no USB keys connected to the enclosure. (Aucune clé USB connectée au boîtier.)

295 No valid firmware images found on USB key. (Aucune image de microprogramme valide trouvée sur la clé USB.)

296 No configuration scripts found on USB key. (Aucun script de configuration trouvé sur la clé USB.)

297 I/O error on USB key. (Erreur E/S sur la clé USB).

298 Badly formatted USB file URL. (URL de fichier USB de format incorrect).

299 Permission problems when accessing USB media. (Problèmes d'autorisation lors de l'accès au support USB).

300 Error uploading to USB media. (Erreur de chargement vers le support USB).

301 An invalid number of GUIDs was passed to the Onboard Administrator. (Un nombre incorrect de GUID a été transmis au module Onboard Administrator.)

302 URL flash image for microcode download not available. (Image flash d'URL de téléchargement de microcode non disponible).

303 Invalid session timeout. (Délai d'expiration de session non valide)

304 Invalid watts value. (Valeur en watts non valide).

305 Failed to store change for power cap. (Échec du stockage de modification de plafond d'alimentation).

306 Enclosure Dynamic Power Cap feature is not allowed. (La fonction de limitation d'alimentation dynamique de boîtier n'est pas autorisée.)

307 Wrong number of bays specified for enclosure while setting capping bays to exclude. (Nombre incorrect de baies spécifié pour boîtier tout en fixant le plafonnement des baies à exclure.)

308 The number of bays opted out exceeds the maximum allowed. (Le nombre de baies retirées dépasse le maximum autorisé.)

309 Enclosure Dynamic Power Cap feature is not allowed. (La fonction de limitation d'alimentation dynamique de boîtier n'est pas autorisée.)

310 Enclosure Dynamic Power Cap is set. (La limitation d'alimentation dynamique de boîtier est définie.)

311 Enclosure Dynamic Power Cap is not set. (La limitation d'alimentation dynamique de boîtier n'est pas définie) Cannot confirm that device tray meets minimum firmware version required. (il est impossible de confirmer que la version minimum requise du microprogramme est installée sur les périphériques.)

312 Enclosure Dynamic Power Cap not set. (La limitation d'alimentation dynamique de boîtier n'est pas définie) Device tray fails to meet the minimum required firmware version. (Le plateau de périphériques ne satisfait pas la version minimum requise du microprogramme.)

313 The requested cap is outside the allowable range of Enclosure Dynamic Power Cap values. (La limitation demandée est en dehors de la plage autorisée des valeurs de limitation d'alimentation dynamique de boîtier.)

314 Server Power Reduction cannot currently be enabled. (La réduction d'alimentation serveur ne peut pas être activée.) Enclosure Dynamic Power Cap is not allowed. (La limitation d'alimentation dynamique de boîtier n'est pas autorisée.)

315 No valid ISO images found on USB key. (Aucune image ISO valide trouvée sur la clé USB).

316 Bay privileges cannot be revoked for Administrators with OA permission. (Impossible de révoquer les privilèges de baie pour les administrateurs avec autorisation OA.)

317 Invalid DNS hostname. (Nom d'hôte DNS non valide).

318 Factory defaults cannot be restored because the enclosure is in VC mode. (Impossible de restaurer les valeurs usine par défaut car le boîtier est en mode VC.)

319 The string entered is not a valid IPv6 address. (La chaîne entrée n'est pas une adresse IPv6 valide.)

320 IPv6 static address already exists. (L'adresse statique IPv6 existe déjà).

321 IPv6 static address not found. (Adresse statique IPv6 introuvable).

322 Unable to add. (Ajout impossible).

323 Invalid SMTP server. (Serveur SMTP non valide).

324 Invalid SNMP Trap receiver. (Récepteur d'interruptions SNMP non valide).

325 Invalid NTP server. (Serveur NTP non valide).

326 Invalid EBIPA configuration. (Configuration EBIPA non valide.) Multiple subnets were detected. (Sous-réseaux multiples détectés.)

327 Specified VLAN ID does not exist. (L'ID VLAN spécifié n'existe pas.)

328 Cannot delete the default VLAN ID. (Impossible de supprimer l'ID VLAN par défaut).

329 Maximum VLAN entries reached. (Nombre d'entrées VLAN maximum atteint).

330 Duplicated VLAN ID. (ID VLAN dupliqué).

331 Specified VLAN ID is invalid. (L'ID VLAN spécifié n'est pas valide.)

332 Operation partially successful. (Opération partiellement réussie).

333 Duplicated VLAN name. (Nom VLAN dupliqué).

334 A pending command already exists. (Une commande en attente existe déjà.)

337 The remote syslog server address cannot be cleared while remote logging is enabled. (L'adresse du serveur syslog distant ne peut pas être effacée à distance alors que la journalisation distante est activée.)

338 Invalid search context number. (Nombre de contextes de recherche non valide).

339 Not on the same VLAN ID domain. (Non sur le même domaine d'ID VLAN).

340 This command is not valid for auxiliary blades. (Cette commande n'est pas valide pour les lames auxiliaires.)

341 No LDAP groups currently exist. (Aucun groupe LDAP n'existe actuellement.)

342 The requested Derated Circuit Capacity is outside the allowable range of values for this enclosure. (La capacité de circuit déclassée est en dehors de la plage de valeurs autorisées pour ce boîtier.)

343 The requested Rated Circuit Capacity is outside the allowable range of values for this enclosure. (La capacité nominale de circuit demandée est en dehors de la plage de valeurs autorisées pour ce boîtier.)

344 The requested cap is greater than the requested Derated Circuit Capacity. (La capacité demandée est supérieure à la capacité de circuit déclassée demandée.)

345 The requested Derated Circuit Capacity is greater than the requested Rated Circuit Capacity. (La capacité de circuit déclassée demandée est supérieure à la capacité nominale de circuit demandée.)

346 The requested set of bays to exclude cause the cap to be outside the allowable range. (L'ensemble demandé de baies à exclure entraîne la limite à se trouver en dehors de la plage autorisée.)

347 The requested set of bays to exclude cause the Derated Circuit Capacity to be outside the allowable range. (L'ensemble demandé de baies à exclure entraîne la capacité de circuit déclassée à se trouver en dehors de la plage autorisée.)

348 The requested set of bays to exclude cause the Rated Circuit Capacity to be outside the allowable range. (L'ensemble demandé de baies à exclure entraîne la capacité nominale de circuit à se trouver en dehors de la plage autorisée.)

353 IPv6 is currently disabled. (IPv6 actuellement désactivé) Cannot download certificate from the specified address. (téléchargement du certificat à partir de l'adresse indiquée impossible.)

354 The date cannot be set to a date in the past. (La date ne peut pas être définie sur une date du passé.)

356 The setting cannot be cleared while LDAP is enabled. (Le paramètre ne peut pas être supprimé si LDAP est activé.)

357 URB reporting using HTTP(S) cannot be enabled until an HTTP(S) endpoint has been configured. (Le signalement URB via HTTP(S) ne peut être activé tant qu'une extrémité n'a pas été configurée.)

358 URB reporting using SMTP cannot be enabled until an SMTP server and mailbox have been configured. (Le signalement URB via SMTP ne peut être activé tant qu'un serveur et une boîte aux lettres SMTP n'ont pas été configurés.)

359 URB reporting using SMTP and HTTP(S) cannot be enabled until HTTP(S) and SMTP settings have been configured. (Le signalement URB via SMTP et HTTP(S) ne peut être activé tant que les paramètres HTTP(S) et SMTP n'ont pas été configurés.)

360 Warning: Not all VC-Enet modules are on the same VLAN ID. (Avertissement : tous les modules VC-Enet ne sont pas sur le même ID VLAN.)

361 File doesn't exist. (Le fichier n'existe pas.)

362 This operation cannot be performed when AlertMail is enabled. (Cette opération ne peut pas être effectuée lorsque AlertMail est activé.)

363 Setting SolutionsId failed. (Échec de la définition de la solution.)

364 SolutionsId must be an 8-byte hex string, between 0000000000000000 and FFFFFFFFFFFFFFFF. (L'identifiant de solution doit être une chaîne hexadécimale à 8 octets comprise entre 0000000000000000 et FFFFFFFFFFFFFFFF.)

365 Failed Remote Support registration (Échec de l'enregistrement à l'assistance à distance).

366 Failed Remote Support un-registration (Échec de l'annulation d'enregistrement à l'assistance à distance).

367 Failed Remote Support restore registration (Échec de la restauration de l'enregistrement à l'assistance à distance).

368 Failed to send Remote Support message (Hint: Check the Remote Support proxy and endpoint URL. Use SET REMOTE_SUPPORT PROXY to configure and re-try.) (Échec de l'envoi de message de support distant (Astuce : Vérifiez le proxy de support distant et l'URL de point de fin. Utilisez SET REMOTE_SUPPORT PROXY pour configurer, puis réessayez.))

369 Failed to set Remote Support interval. Valid interval is 0 to 60 (days) Intervalle valide : 0 à 60 jours.)

370 You must configure the directory server and SSL port before testing LDAP. (Vous devez configurer le serveur d'annuaires et le port SSL avant de tester LDAP.)

371 The string contains an invalid character. (La chaîne contient un caractère non valide.)

372 This operation cannot be performed when Remote Support is disabled. (Cette opération ne peut pas être effectuée lorsque l'assistance à distance est désactivée.)

373 Cannot set Maintenance Mode Timeout. (Définition du délai d'expiration de maintenance impossible.) Value should be between 5 minutes and 2 weeks. (La valeur doit être comprise entre 5 minutes et 2 semaines.)

374 Insert eRs error here. (Insérer erreur eR à cet endroit.)

375 The string entered is not a valid LDAP server. (La chaîne entrée ne correspond pas à un serveur LDAP valide.) A LDAP server must be a IP address or DNS name. (Un serveur LDAP est une adresse IP ou un nom DNS.)

376 Unable to perform the operation. (Impossible d'effectuer l'opération.) Retry the operation or restart OA. (Recommencez l'opération ou redémarrez OA) (System Error 376) (Erreur système 376)

377 The HP Passport credentials provided are invalid. (Les informations de connexion HP Passport ne sont pas valides.)

378 This system is already registered. (Ce système est déjà enregistré.)

379 Please disable Remote Support before performing this action. (Veuillez désactiver l'assistance à distance avant d'exécuter cette action.)

380 Transaction UUID is mismatched. (L'identifiant UUID de la transaction ne correspond pas.)

381 Unable to download ilo flash image from the url provided. (Téléchargement de l'image flash ILO impossible à partir de l'URL fournie.) Supported protocols are http, https, tftp and ftp. (Les protocoles pris en charge sont http, https, tftp et ftp.)

382 The Onboard Administrator is still initializing. (Onboard Administrator en cours d'initialisation.) Please try your request again later. (Veuillez réessayer ultérieurement.)

383 Failed to send Remote Support message. (Échec de l'envoi du message à l'assistance à distance.) Vérifiez que DNS est activé et vérifiez l'hôte de Insight Remote Support et les informations de port.

384 Failed to resolve HP Insight Remote Support hosting server. (Impossible de résoudre le serveur d'hébergement de HP Insight Remote Support.) Please verify DNS settings and Insight Remote Support host and port information. (Vérifiez les paramètres DNS, l'hôte de Insight Remote Support et les informations de port).

385 Transmission to the HP Insight Remote Support receiver was unsuccessful. (La transmission vers le récepteur de HP Insight Remote Support a échoué.) Please check connectivity between the OA and the Insight Remote Support receiver. (Vérifiez la connectivité entre OA et le récepteur de Insight Remote Support.)

389 This action cannot be performed in FIPS MODE ON/DEBUG. (Cette action ne peut être effectuée en MODE FIPS ON/DEBUG)

391 No Variable Name-Value pairs are provided for substitution. (Pas de paires Nom variable-valeur fournies pour remplacement.)

392 Attempted to substitute more than 25 variables. (Tentative de remplacement de plus de 25 variables.)

395 Trying to substitute the same variable twice. (Tentative de remplacement de la même variable à deux reprises.)

396 String_list searchFlag out of range. (String_list searchFlag hors plage.)

397 No variable names are passed in for searching. (Pas de noms de variables pour la recherche.)

398 No variable values are passed in for searching. (Pas de valeurs de variables pour la recherche.)

401 Enclosure Firmware Management is currently disabled. (La gestion du microprogramme du boîtier est actuellement désactivée.)

402 The Enclosure Firmware Management ISO URL is not set. (L'URL ISO de gestion du microprogramme du boîtier n'est pas définie.)

403 This operation cannot be performed when Enclosure Firmware Management is running. (Cette opération ne peut pas être effectuée lorsque la gestion de microprogramme de boîtier est en cours d'exécution.)

404 Unable to mount ISO or validate version information. (Montage ISO ou validation des informations de version impossible.)

Check URL and validate ISO is available from URL entered. (Vérifiez que l'URL et la validation sont disponibles à partir de l'URL entrée.)

405 Unable to open firmware log. (Ouverture du journal de microprogramme impossible.)

406 The blade's firmware has not been discovered. (Le microprogramme de lame n'a pas été détecté.)

407 An error occurred while reading the firmware log. (Une erreur s'est produite lors de la lecture du journal du microprogramme.)

408 Enclosure Firmware Management is not supported by this device type. (La gestion de microprogramme du boîtier n'est pas prise en charge par ce type de périphérique.)

409 Firmware ISO image is in use, changing url is not allowed. (Image ISO du microprogramme en cours d'utilisation, changement d'URL non autorisé.)

410 Blade must be powered off before starting Enclosure Firmware Management. (La lame doit être mise hors tension avant le démarrage de la gestion de microprogramme du boîtier.)

411 Unable to change passwords for any LDAP or HPSIM users. (Modification des mots de passe des utilisateurs LDAP ou HPSIM impossible.)

412 Enclosure Firmware Management is not available. (Gestion du microprogramme de boîtier non disponible.) To use this feature, it needs to be unlocked. (Déverrouillez la fonction pour pouvoir l'utiliser.)

413 Enclosure Firmware Management is not supported on the Active OA hardware present. (Gestion du microprogramme de boîtier non prise en charge sur le matériel OA actif présent.)

414 Could not persist firmware management log. (Poursuite du journal de gestion du microprogramme impossible.)

415 When in FIPS MODE ON/DEBUG, the password length must be between 8 and 40 characters. (En mode FIPS ON/DEBUG, la longueur du mot de passe doit être définie entre 8 et 40 caractères.)

416 When in FIPS MODE ON/DEBUG, strict passwords must be enabled. (En mode FIPS ON/DEBUG, des mots de passe stricts doivent être activés.)

417 Certificate hash algorithm is not supported. (L'algorithme de hachage de certificat n'est pas pris en charge.) See OA syslog for more information. (Consultez syslog OA pour plus d'informations.)

418 Downgrade is not allowed in FIPS mode ON/DEBUG. (La dégradation n'est pas autorisée en mode FIPS ON/DEBUG.) Please set FIPS mode to OFF and retry the operation. (Veuillez définir le mode FIPS sur OFF et recommencer l'opération.)

419 Could not persist firmware management log. (Poursuite du journal de gestion du microprogramme impossible.)

427 E-Keying busy. (E-Keying occupé.)

428 Error getting CLP strings. (Erreur d'obtention des chaînes CLP.)

431 Enclosure Firmware Management is not ready, please try again in a few minutes. (La gestion du microprogramme du boîtier n'est pas prête, essayez de nouveau dans quelques minutes.)

434 PIN Protection cannot be disabled in FIPS Mode. (La protection PIN ne peut pas être désactivée en mode FIPS.)

435 Cannot restore the factory defaults while in FIPS mode. (Impossible de restaurer les paramètres par défaut en mode FIPS.)

437 Bad EBIPAv6 device. (Périphérique EBIPAv6 incorrect.)

438 An EBIPAv6 configuration error occurred. (Une erreur de configuration EBIPA s'est produite.) Extended information is available as a bitcode reason code. (Les informations étendues sont disponibles en tant que motif de code binaire.)

439 Invalid hash algorithm. (Algorithme de hachage non valide.) The hash algorithm must be one of: SHA1, SHA-224, SHA-256, SHA-384, or SHA-512. (L'algorithme de hachage doit correspondre à : SHA1, SHA-224, SHA-256, SHA-384 ou SHA-512.)

440 You must set a new pin code before unlocking the LCD buttons. (Vous devez définir un nouveau code PIN avant de déverrouiller les touches LCD.)

441 The requested operation cannot be completed during a firmware update. (L'opération demandée ne peut être réalisée au cours d'une mise à jour du microprogramme.)

442 This enclosure is incapable of performing a reset on a non-redundant Onboard Administrator. (Ce boîtier ne peut pas effectuer une réinitialisation sur un module Onboard Administrator non redondant.)

444 Power cap configuration locked due to active group management. (La configuration du condensateur de puissance est verrouillée en raison de la gestion de groupe active.)

REMOTE SUPPORT TIER2

445 HP Remote Support receiver temporarily unavailable. (Le récepteur de HP Remote Support est temporairement indisponible.) Please retry later. (Réessayez plus tard.)

446 Unregistration request was not processed successfully by the HP Remote Support receiver. (La demande d'annulation d'inscription n'a pas été traitée avec succès par le récepteur de HP Remote Support.) Remote Support has been disabled locally. (Remote Support a été désactivé localement.) Aucun événement lié au service ni aucune donnée ne seront envoyés jusqu'à ce périphérique ait été réinscrit.

447 Authentication error. (Erreur d'authentification.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

448 Missing device identifiers. (Identifiants du périphérique manquants.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

449 Corrupt device identifiers. (Identifiants du périphérique corrompus.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

450 Insufficient device identifier information. (Informations sur l'identifiant du périphérique insuffisantes.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

451 Invalid device identifier information. (Informations sur l'identifiant du périphérique non valides.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

452 Stale device identifiers. (Identifiants du périphérique périmés) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

453 Missing GDID. (GDID manquant.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

454 Corrupt GDID. (GDID corrompu.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

455 Missing registration token. (Jeton d'inscription manquant.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

456 Corrupt registration token. (Jeton d'inscription corrompu.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

457 Expired registration token. (Jeton d'inscription expiré.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

458 Invalid HP Passport credentials. (Informations d'identification HP Passport non valides.) Please verify and enter valid HP Passport account credentials. (Vérifiez et entrez des identifiants de compte HP Passport valides.)

459 Device is already registered. (Le périphérique est déjà inscrit.) Please delete the device from Insight Remote Support user interface and retry registration. (Supprimez le périphérique de l'interface utilisateur de HP Insight Remote Support, puis renouvelez l'inscription.)

460 Unknown device. (Périphérique inconnu.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

461 Insufficient registration data. (Données d'inscription insuffisantes.) Please retry registration. (Renouvelez l'inscription.)

462 Missing SOAP header. (En-tête SOAP manquant.) Please retry your last step. (Recommencez la dernière étape.) If error persists and device is currently registered, unregister and re-register device. (Si l'erreur persiste et que le périphérique est actuellement inscrit, procédez à sa désinscription, puis réinscrivez-le.)

463 Missing GUID. (GUID manquant.) Please retry your last step. (Réessayez la dernière étape.) If error persists and device is currently registered, unregister and re-register device. (Si l'erreur persiste et que le périphérique est actuellement inscrit, procédez à sa désinscription, puis réinscrivez-le.)

464 Corrupt GUID. (GUID corrompu.) Please retry your last step. (Réessayez la dernière étape.) If error persists and device is currently registered, unregister and re-register device. (Si l'erreur persiste et que le périphérique est actuellement inscrit, procédez à sa désinscription, puis réinscrivez-le.)

465 Missing data package. (Package de données manquant.) Please retry your last step. (Réessayez la dernière étape.) If error persists and device is currently registered, unregister and re-register

device. (Si l'erreur persiste et que le périphérique est actuellement inscrit, procédez à sa désinscription, puis réinscrivez-le.)

466 Data Package validation failed. (Échec de la validation du package de données.) Please retry your last step. (Réessayez la dernière étape.) If error persists and device is currently registered, unregister and re-register device. (Si l'erreur persiste et que le périphérique est actuellement inscrit, procédez à sa désinscription, puis réinscrivez-le.)

467 HP Passport password must be changed or reset. (Le mot de passe HP Passport doit être changé ou réinitialisé.) Please attempt to register again after correcting the HP Passport account issue. (Essayez de vous enregistrer de nouveau après la correction du problème de compte HP Passport.)

468 Expired HP Passport credentials. (Informations d'identification HP Passport expirées.) Please attempt to register again after correcting the HP Passport account issue. (Essayez de vous enregistrer de nouveau après la correction du problème de compte HP Passport.)

469 HP Passport account locked out. (Compte HP Passport verrouillé.) Please attempt to register again after correcting the HP Passport account issue. (Essayez de vous enregistrer de nouveau après la correction du problème de compte HP Passport.)

470 GDID and device identifiers do not match. (Les identifiants GDID et ceux du périphérique ne correspondent pas.) If error persists and device is not currently registered, unregister and re-register device. (Si l'erreur persiste et que le périphérique n'est pas inscrit, procédez à sa désinscription, puis réinscrivez-le.)

471 Device is not registered. (Le périphérique n'est pas inscrit.) Remote Support registration has been disabled locally on this device. (L'inscription à Remote Support a été désactivée localement sur ce périphérique.) No service events or data collections will be sent until this device has been re-registered. (Aucun événement lié au service ni aucune donnée ne seront envoyés jusqu'à ce périphérique ait été réinscrit.)

472 Deleted device. (Périphérique supprimé.) This device has been previously deleted from the Insight Remote Support user interface. (Ce périphérique a été précédemment supprimé de l'interface utilisateur d'Insight Remote Support.) Please unregister and re-register device. (Procédez à la désinscription, puis réinscrivez le périphérique.)

473 Unhandled error. (Erreur non gérée.)

474 Failed to connect to HP Insight Remote Support direct connect web service. (Impossible de se connecter au service Web de connexion directe de HP Insight Remote Support.) Please verify DNS settings, proxy settings and connectivity. (Vérifiez les paramètres DNS, les paramètres du proxy et la connectivité.)

475 Dynamic DNS is not enabled. (DNS dynamique n'est pas activée.)

476 Invalid SNMP Engine ID. (Identifiant de moteur SNMP non valide.) The Engine ID must start with '0x' followed by an even number of up to 64 hexadecimal digits. (L'identifiant de moteur doit commencer par « 0x » suivi par un nombre pair contenant jusqu'à 64 chiffres hexadécimaux.)

477 Invalid Authentication Protocol. (Protocole d'authentification non valide.)

478 Invalid Authentication Password, must contain 8 to 40 printable characters. (Mot de passe d'authentification non valide, doit contenir entre 8 et 40 caractères imprimables.)

479 Invalid Privacy Protocol. (Protocole de confidentialité non valide.)

480 Invalid Privacy Password, must contain 8 to 40 printable characters. (Mot de passe de confidentialité non valide, doit contenir entre 8 et 40 caractères imprimables.)

481 Duplicate user, a SNMP user by this name and engine id already exists. (Utilisateur dupliqué, un utilisateur SNMP avec ce nom et cet identifiant de moteur existe déjà.)

482 Invalid minimal security setting. (Paramètre de sécurité minimale non valide.)

483 Invalid security setting. (Paramètre de sécurité non valide.)

484 Selected algorithm cannot be used while FIPS mode is enabled. (Impossible d'utiliser l'algorithme sélectionné lorsque le mode FIPS est activé.)

485 A user with read-write access cannot be created while FIPS mode is enabled. (Impossible de créer un utilisateur avec un accès en lecture-écriture lorsque le mode FIPS est activé.)

486 You cannot use a remote engine id with a trap. (Vous ne pouvez pas utiliser d'identifiant de moteur à distance avec une interruption.)

487 You cannot use the local engine id with an inform. (Vous ne pouvez pas utiliser d'identifiant de moteur local avec une interruption.)

489 Error adding the language pack. (Erreur d'ajout du pack de langues.)

490 Error removing the language pack. (Erreur de suppression du pack de langues.)

491 The file provided is not a valid Onboard Administrator language pack image. (Le fichier fourni n'est pas une image de pack de langues Onboard Administrator valide.)

492 Cannot remove the English language pack. (Impossible de supprimer le pack de langues.)

493 The language support pack is not installed. (Le pack de prise en charge linguistique n'est pas installé.)

494 The submitted file is not a valid SSH key. (Le fichier présenté n'est pas une clé SSH valide.)

499 The firmware image provided doesn't meet the VC Minimum Firmware Version requirement. (L'image du microprogramme fournie ne répond pas à l'exigence minimum de version du microprogramme VC.) Check the OA Syslog for more details. (Vérifiez le Syslog OA pour plus de détails.)

500 The action did not complete successfully. (L'action n'a pas abouti.)

502 Invalid response. (Réponse non valide.) No connection or network busy. (Pas de connexion ou réseau occupé.)

503 Web server busy or in service. (Serveur Web occupé ou en service)

510 Remote Support services are provided by other solution. (Les services Remote Support sont fournis par une autre solution.)

511 DHCP-Supplied Domain Name cannot be disabled when the user-supplied domain name is not set. (Le nom de domaine fourni via DHCP ne peut pas être désactivé lorsque le nom de domaine fourni par l'utilisateur n'est pas défini.)

512 The text must contain at least one visible character. (Le texte doit contenir au moins un caractère visible.)

514 User ID is a required field. (L'identifiant de l'utilisateur est un champ obligatoire.) Please retry registration. (Renouvelez l'inscription.)

515 The user must have an active authenticated session. (L'utilisateur doit avoir une session active authentifiée.) Please retry registration. (Renouvelez l'inscription.)

516 HP Passport system failure occurred. (Une défaillance du système HP Passport s'est produite.) A problem has been detected in the HP Passport system. (Un problème a été détecté dans le système HP Passport.) Please retry later. (Réessayez plus tard.)

517 The session token is invalid due to any of the following reasons: failed decoding, token is null or empty, userId is empty or session start value is not a number. (Le jeton de session est non valide pour l'une des raisons suivantes : décodage défaillant, un jeton est nul ou vide, userId est vide ou la valeur de démarrage de session n'est pas un nombre.) Please retry registration. (Renouvelez l'inscription.)

518 Password required. (Mot de passe requis.) Please retry registration. (Renouvelez l'inscription.)

519 HP Passport user ID is invalid. (L'identifiant d'utilisateur HP Passport n'est pas valide.) Please retry registration with a valid user ID. (Renouvelez l'inscription avec un identifiant utilisateur valide.)

520 HP Passport account is locked out due to excessive login authentication failures. (Le compte HP Passport est verrouillé en raison d'échecs d'authentification de connexion excessifs.) Please reset your password and retry registration. (Réinitialisez votre mot de passe et recommencez l'inscription.)

521 User has reached half the maximum allowed HP Passport login authentication failures. (L'utilisateur a atteint la moitié du maximum autorisé d'échecs d'authentification de connexion HP Passport.) Please verify your username and password are correct and retry registration. (Vérifiez si votre nom d'utilisateur et votre mot de passe sont corrects et recommencez l'inscription.)

522 HP Passport password has expired. (Le mot de passe HP Passport a expiré.) Please update your password and retry registration. (Mettez à jour votre mot de passe et recommencez l'inscription.)

523 User has at least one of the HP Passport required on-line identity elements missing. (L'utilisateur a au moins un élément d'identité en ligne requis par HP Passport manquant.) Please update your HP Passport profile and retry registration. (Mettez à jour votre profil HP Passport et recommencez l'inscription.)

524 HP Passport Security Q and A is not compliant; the user must enter a new security Q and A upon login. (La question et la réponse de sécurité de HP Passport ne sont pas conformes, l'utilisateur doit les entrer à nouveau au moment de la connexion.) Please update your HP Passport security Q and A and retry registration. (Mettez à jour votre question et votre réponse de sécurité HP Passport et recommencez l'inscription.)

525 HP Passport password entered is incorrect. (Le mot de passe HP Passport saisi est incorrect.) Please retry registration using the correct password. (Recommencez l'inscription avec le mot de passe correct.)

526 HP Passport user has been added to a group. (L'utilisateur HP Passport a été ajouté à un groupe.) Please reset your password and retry registration. (Réinitialisez votre mot de passe et recommencez l'inscription.)

527 User must enter an HP Passport security Q and A and change password. (L'utilisateur doit entrer une question et une réponse de sécurité HP Passport et modifier son mot de passe.) Please update your security Q and A, update your password, and retry registration. (Mettez à jour votre question et votre réponse de sécurité et recommencez l'inscription.)

528 Protocol error occurred while communicating with the HP Insight Remote Support receiver. (Une erreur de protocole s'est produite lors de la communication avec le récepteur de HP Insight Remote Support.)

529 Failed to resolve proxy. (Impossible de résoudre le proxy.) Please verify DNS settings, proxy settings and connectivity. (Vérifiez les paramètres DNS, les paramètres du proxy et la connectivité.)

530 Failed to connect to the HP Insight Remote Support hosting server. (Impossible de se connecter au serveur d'hébergement de HP Insight Remote Support.) Please verify Insight Remote Support host and port information. (Vérifiez l'hôte de Insight Remote Support et les informations de port.)

531 Failed to connect to the HP Insight Remote Support direct connect web service. (Impossible de se connecter au service Web de connexion directe de HP Insight Remote Support.) Please verify

DNS settings, proxy settings and connectivity. (Vérifiez les paramètres DNS, les paramètres du proxy et la connectivité.)

532 HP Remote Support receiver protocol error. (Erreur de protocole du récepteur de HP Remote Support.)

533 The setting cannot be cleared when user domain name is enabled. (Impossible d'effacer le paramètre lorsque le nom de domaine de l'utilisateur est activé.)

534 The operation cannot be performed while Enclosure Firmware Management is enabled. (L'opération ne peut pas être effectuée lorsque la gestion de microprogramme de boîtier est activée.)

535 Invalid SNMP Engine ID string. (Chaîne d'identifiant de moteur SNMP non valide). The Engine ID string must contain 1 to 27 printable characters. (La chaîne de l'identifiant de moteur doit contenir entre 1 et 27 caractères imprimables.)

536 The password is too short. (Le mot de passe est trop court.)

537 The password is too long. (Le mot de passe est trop long.)

538 Error installing the certificate. (Erreur lors de l'installation du certificat.)

539 Enclosure IP mode requires the active Onboard Administrator to have a static IPv4 address or a static IPv6 address. (Le mode IP de boîtier requiert que le module Onboard Administrator actif dispose d'une adresse IPv4 statique ou d'une adresse IPv6 statique.) If IPv6 is not enabled, only the static IPv4 address can be used. (Si IPv6 n'est pas activé, seule l'adresse IPv4 statique peut être utilisée.)

540 Configure a static IPv6 address for your active OA or disable Enclosure IP Mode before enabling DHCP for IPv4. (Configurez une adresse IPv6 statique pour votre OA actif ou désactivez le mode IP du boîtier avant d'activer DHCP pour IPv4.)

541 Configure a static IPv4 address for your active OA or disable Enclosure IP Mode before disabling IPv6. (Configurez une adresse IPv4 statique pour votre OA actif ou désactivez le mode IP du boîtier avant de désactiver IPv6.)

542 The submitted URL is invalid for uploading. (L'URL soumise n'est pas valide pour le téléchargement.)

543 This version of Onboard Administrator firmware does not support boot options for servers configured in UEFI boot mode. (Cette version du microprogramme de Onboard Administrator ne prend pas en charge les options de démarrage pour les serveurs configurés en mode de démarrage UEFI.)

544 This operation cannot be performed while Secure Boot is enabled. (Cette opération ne peut pas être effectuée lorsque Secure Boot est activé.)

545 This operation cannot be performed while Secure Boot is enabled or blade is booting the OS. (Cette opération ne peut pas être effectuée lorsque Secure Boot est activé ou que la lame démarre le système d'exploitation.)

561 Transmission from the HP Insight Remote Support receiver was unsuccessful. (La transmission à partir du récepteur de HP Insight Remote Support a échoué.)

562 Transmission from the HP Insight Remote Support receiver was unsuccessful. (La transmission à partir du récepteur de HP Insight Remote Support a échoué.) Please check connectivity between OA and the Insight Remote Support receiver. (Vérifiez la connectivité entre OA et le récepteur Insight Remote Support.)

563 The key strength for the provided key is invalid for this configuration. (La puissance de la clé fournie n'est pas valide pour cette configuration.)

564 This command is not supported by the interconnect. (Cette commande n'est pas prise en charge par l'interconnexion.)

565 The string entered is a link-local address and cannot be used for assignment. (La chaîne entrée n'est une adresse de liaison locale et ne peut pas être utilisée pour l'affectation.)

566 Invalid IPv6 static route gateway. (Passerelle de route statique IPv6 non valide.) Route gateway must not be empty and must not contain prefix length. (La passerelle de route ne doit pas être vide et ne doit pas contenir de longueur de préfixe.)

567 IPv6 static route destination already exists. (La destination de route statique IPv6 existe déjà.)

568 Unable to add IPv6 route. (Impossible d'ajouter une route IPv6.) The maximum number of IPV6 static routes already exist. (Le nombre maximum de routes statiques IPV6 existe déjà.)

569 IPv6 static route not found. (Route statique IPv6 introuvable.)

570 Invalid IPv6 static route destination. (Destination de route statique IPv6 non valide.) The route destination must be a valid IPv6 address. (La destination de route doit être une adresse IPv6 valide.)

571 All items cannot be disabled. (Tous les articles ne peuvent pas être désactivés.)

572 This action requires the OA to be in FIPS Mode ON/DEBUG. (Cette action nécessite que le module OA soit en mode FIPS ON/DEBUG.)

573 Must set MINRATE option if using timeout range. (Doit définir l'option MINRATE en cas d'utilisation de plage de délai d'expiration.)

574 Minimum data rate must be larger than 0. (Le taux de données minimum doit être supérieur à 0.)

575 Maximum timeout must be larger than minimum timeout. (Le délai d'expiration maximum doit être supérieur au délai d'expiration minimum.)

576 Timeout must be larger than 0. (Le délai d'expiration doit être supérieur à 0.)

577 HTTP Read Timeout is already set to the requested value. (Le délai d'attente de lecture HTTP est déjà défini sur la valeur demandée.)

Erreurs de capture d'écran Insight Display

1 Missing credentials. (Informations de connexion manquantes.)

2 The getLCDImage CGI process has caught the SIGSEGV signal. (Le processus CGI getLCDImage a détecté le signal SIGSEGV.)

3 Could not acquire access to the image in a reasonable amount of time. (Impossible d'acquérir un accès à l'image dans un délai raisonnable.)

4 Cannot open semaphores. (Impossible d'ouvrir des sémaphores.)

5 Produce SEMV does not work. (La production SEMV ne fonctionne pas.)

6 Consume SEMV does not work. (La consommation SEMV ne fonctionne pas.)

7 Cannot lock the image file. (Impossible de verrouiller le fichier d'image.)

8 Cannot open the image file. (Impossible d'ouvrir le fichier d'image.)

9 Cannot seek in the image file. (Impossible de rechercher dans le fichier d'image.)

10 Unable to resume session. (Impossible de reprendre la session)

11 Insufficient privileges. (Privilèges insuffisants.)

Paramètres usine par défaut du module Onboard Administrator

Lorsque vous réinitialisez le HP BladeSystem Onboard Administrator sur les paramètres usine par défaut, le mot de passe de l'administrateur n'est pas réinitialisé sur ces valeurs. Il reste défini sur le dernier mot de passe spécifié. Si le mot de passe de l'administrateur doit être réinitialisé sur les paramètres usine par défaut (comme indiqués sur l'étiquette fournie avec le module Onboard Administrator), passez à la section « Récupération du mot de passe administrateur » (Récupération du mot de passe administrateur à la page 14) de ce manuel.

La réinitialisation du module Onboard Administrator sur les valeurs usine par défaut réinitialise également tous les certificats sur le module Onboard Administrator.

Interruptions SNMP du module Onboard Administrator

Le BladeSystem Onboard Administrator prend en charge les interruptions SNMP suivantes.

ID d'interruption	Nom d'interruption	Description
22001	cpqRackNameChanged	Le nom du rack a changé
22002	cpqRackEnclosureNameChanged	Le nom du boîtier a changé
22003	cpqRackEnclosureRemoved	Retrait de boîtier lié détecté
22004	cpqRackEnclosureInserted	Insertion de boîtier lié détectée
22008	cpqRackEnclosureFanFailed	Le ventilateur de boîtier est défaillant
22009	cpqRackEnclosureFanDegraded	Le ventilateur de boîtier est dégradé
22010	cpqRackEnclosureFanOk	Ventilateur de boîtier OK
22011	cpqRackEnclosureFanRemoved	Retrait du ventilateur de boîtier
22012	cpqRackEnclosureFanInserted	Insertion du ventilateur de boîtier
22013	cpqRackPowerSupplyFailed	Le bloc d'alimentation de boîtier est en panne
22014	cpqRackPowerSupplyDegraded	Le bloc d'alimentation de boîtier est dégradé
22015	cpqRackPowerSupplyOk	Le bloc d'alimentation de boîtier est OK
22016	cpqRackPowerSupplyRemoved	Le bloc d'alimentation de boîtier est retiré
22017	cpqRackPowerSupplyInserted	Le bloc d'alimentation de boîtier est inséré
22018	cpqRackPowerSubsystemNotRedundant	Le sous-système d'alimentation de boîtier n'est pas redondant
22019	cpqRackPowerSubsystemLineVoltageProblem	Problème de tension de ligne de sous-système d'alimentation de boîtier
22020	cpqRackPowerSubsystemOverloadCondition	Condition de surcharge de sous-système d'alimentation de boîtier
22028	cpqRackServerBladeRemoved	Lame retirée (remplacé par 22050 dans OA v1.30)
22029	cpqRackServerBladeInserted	Lame insérée (remplacé par 22051 dans OA v1.30)
22037	cpqRackEnclosureManagerDegraded	Module Onboard Administrator dégradé

ID d'interruption	Nom d'interruption	Description
22038	cpqRackEnclosureManagerOk	Module Onboard Administrator OK
22039	cpqRackEnclosureManagerRemoved	Module Onboard Administrator retiré
22040	cpqRackEnclosureManagerInserted	Module Onboard Administrator inséré
22041	cpqRackManagerPrimaryRole	Le module Onboard Administrator est actif
22042	cpqRackServerBladeEKeyingFailed	Échec de configuration eKeying de lame
22044	cpqRackNetConnectorRemoved	Module d'interconnexion retiré
22045	cpqRackNetConnectorInserted	Module d'interconnexion inséré
22046	cpqRackNetConnectorFailed	Module d'interconnexion défectueux
22047	cpqRackNetConnectorDegraded	Module d'interconnexion dégradé
22048	cpqRackNetConnectorOk	Module d'interconnexion OK
22049	cpqRackServerBladeToLowPower	La lame a demandé une puissance trop basse
22050	cpqRackServerBladeRemoved2	Lame retirée2
22051	cpqRackServerBladeInserted2	Lame insérée2
22083	cpqRackEnclosureManagerLinkDown	Lien réseau Onboard Administrator en Standby inactif
22084	cpqRackEnclosureManagerLinkUp	Lien réseau Onboard Administrator en Standby actif
22085	cpqRackErsCommFailure	Échec de communication du module Onboard Administrator vers un support à distance
22086	cpqRackPowerSubsystemOverloadConditionRepaired	Condition de surcharge de sous-système d'alimentation de boîtier résolue

Problèmes connus liés au navigateur

- **Problèmes généraux d'accès à des applications à partir de liens fournis par l'interface utilisateur du module Onboard Administrator**

  Pour qu'une application de gestion fonctionne correctement lorsque vous y accédez à partir d'un lien Onboard Administrator, vous pouvez avoir à ajouter le domaine Onboard Administrator à vos sites de confiance. En outre, notez que les applications de gestion ouvertes par les liens peuvent ne pas prendre en charge les mêmes versions de navigateur prises en charge par le module Onboard Administrator.

- **Les connexions au module Onboard Administrator échouent via Internet Explorer et Windows 2003 Active Directory**

  Le module OA 4.30 ne prend plus en charge plusieurs suites de chiffrements en raison de la faiblesse généralement reconnue des algorithmes de chiffrement associés. Pour établir une connexion réussie au module Onboard Administrator, les clients doivent prendre en charge une ou plusieurs des suites de chiffrements répertoriées dans le tableau suivant. Les tentatives de connexion via Internet Explorer et Windows 2003 Active Directory échoueront car cette version de Windows ne possède pas une prise en charge par défaut d'au moins une des suites de chiffrements prises en charge. Vous pouvez ajouter la prise en charge nécessaire en installant et en activant des suites de chiffrements basées sur AES dans Windows 2003. Consultez le

correctif Microsoft disponible sur le site Web de Microsoft Support (http://support.microsoft.com/kb/948963).

Suites de chiffrements SSL/TLS	Noms standard pour suites de chiffrements SSL/TLS
EDH-RSA-DES-CBC3-SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
DHE-RSA-AES128-SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
DHE-RSA-AES256-SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256

- **Problèmes liés à Mozilla Firefox 3.6 (ou version ultérieure)**

  Si vous utilisez Mozilla Firefox 3.6 ou une version supérieure, une pression sur la touche Echap a pour effet de déconnecter toute connexion XMLHttpRequest ouverte, entraînant ainsi un comportement inattendu du client. Pour plus d'informations, reportez-vous à l'article sur Mozilla (https://bugzilla.mozilla.org/show_bug.cgi?id=614304).

- **Problèmes liés au navigateur sur systèmes d'exploitation antérieurs à 2004**

  Les navigateurs sur des systèmes d'exploitation antérieurs à 2004 qui ne disposent pas des derniers correctifs et mises à jour liés à la sécurité et appliqués peuvent ne pas être en mesure de se connecter à l'interface Web Onboard Administrator. Le module Onboard Administrator 3.70 a changé l'algorithme de hachage de certificat par défaut de SHA1 en SHA256. Le support SHA256 n'était généralement pas disponible jusqu'après 2003. Assurez-vous que les exigences minimales suivantes de chaque système d'exploitation sont conçues pour prendre en charge SHA256 :

  - Windows XP nécessite SP3.
  - Windows 2003 Server SP2 nécessite une mise à jour pour prendre en charge SHA256. Pour plus d'informations, consultez le site Web de Microsoft Support (http://support.microsoft.com/kb/968730).
  - Red Hat 4 était à l'origine livré avec OpenSSL 0.9.7 qui ne prend pas en charge SHA256. Mettez à jour le système d'exploitation avec le RPM approprié pour utiliser OpenSSL 0.9.8 ou version ultérieure.

- **Certains navigateurs sont dans l'impossibilité d'accéder au module Onboard Administrator si le certificat du module Onboard Administrator est généré à l'aide de SHA-224 en tant que signature de hachage SSL**

  - OA version 3.70 ou ultérieure permet de changer l'algorithme de signature de hachage. Si un certificat SHA1 est nécessaire dans votre infrastructure réseau, utilisez la commande `GENERATE KEY` du module Onboard Administrator pour modifier la taille de la clé et l'algorithme de hachage.

REMARQUE : Lorsque vous travaillez sur une plate-forme Windows, il est possible que certains navigateurs (tels que Microsoft Internet Explorer et Google Chrome) ne puissent pas accéder à l'interface Web du module Onboard Administrator (version 3.70 ou ultérieure), si le certificat Onboard Administrator a été généré avec SHA-224 en tant que signature de hachage SSL. SHA-224 n'est pas la fonction de hachage par défaut pour les certificats auto-signés du module Onboard Administrator. Par défaut, le module Onboard Administrator utilise le hachage SHA-256 pour les certificats auto-signés.

Le navigateur Mozilla Firefox peut accéder à l'interface Web de ces versions du module Onboard Administrator par l'intermédiaire d'un certificat généré avec SHA-224 en tant que signature de hachage SSL.

- Impossible d'accéder à OA en utilisant un navigateur comme Internet Explorer et Google Chrome lorsque les clés sont générées avec SSL et l'algorithme de hachage SHA-224 à partir de OA version 3.70 à 4.50.

REMARQUE : Les navigateurs Microsoft Internet Explorer, Google Chrome et Safari ne peuvent pas accéder à l'interface Web du module Onboard Administrator si le certificat du module Onboard Administrator est généré avec SHA-224 en tant que signature SSL de hachage lors de l'exécution sur Windows XP, Windows Vista et Windows 7. SHA-224 n'est pas la fonction de hachage par défaut pour les certificats auto-signés du module Onboard Administrator.

- **Certains navigateurs ne prennent pas en charge la notation « %scope_id" » avec une adresse locale de liaison IPv6 : certaines fonctionnalités Onboard Administrator sont perdues lorsque l'adresse est utilisée**

  Certains navigateurs ne prennent pas en charge la notation "%scope_id" avec une adresse de liaison locale IPv6. Certains navigateurs peuvent accepter une adresse Web à l'aide de cette notation, mais certaines fonctions peuvent être perdues lorsque l'adresse est utilisée pour accéder au module Onboard Administrator. Les fonctions affectées de l'interface utilisateur du module Onboard Administrator incluent Insight Display et les fonctions de rassemblement de la configuration de l'écran **Configuration Scripts** (**SHOW CONFIG**) et **SHOW ALL**.

- **Google Chrome v27.0.1453.94 ne fonctionne pas correctement avec le module Onboard Administrator 4.01**

  Chrome s'arrête au chargement d'images. D'autres contenus tels que les scripts se chargent correctement. Pour plus de détails, consultez le rapport de problème de Google (http://code.google.com/p/chromium/issues/detail?id=244043).

- **Google Chrome v43.0.2357.10 à v44.0.2383 ne fonctionne pas correctement avec le module Onboard Administrator**

  Si l'utilisateur essaie de se connecter depuis une de ces versions de Chrome, la connexion est autorisée, mais l'interface graphique OA n'affiche pas les informations et n'accepte pas les entrées de l'utilisateur. Pour plus de détails, consultez le rapport de problème Google (https://code.google.com/p/chromium/issues/detail?id=469185).

Problèmes de réseau connus

- **Avec un microprogramme Emulex antérieur à la version 4.1.450.7, DCC n'est pas disponible avec un lien physique de 10 Gb**

  Un problème avec le microprogramme Emulex de version antérieure à la version 4.1.450.7 peut entraîner l'indisponibilité de DCC avec un lien physique de 10 Gb. Lorsque ce problème existe pour des lames de serveur Gen8 et G7 pleine hauteur (y compris les modèles HP ProLiant BL680 G7, BL685c G7, BL620 G7 et BL660 Gen8) avec des cartes HP NC55x LOM ou

FlexibleLOM FLB554 configurées dans un environnement Virtual Connect, une perte de connectivité réseau peut se produire lors de la mise à jour du microprogramme OA à partir de la version 3.56 ou antérieure à la version 3.60 ou ultérieure.

Pour éviter les pertes de connectivité réseau au cours de la mise à jour du microprogramme du module Onboard Administrator, avant d'effectuer la mise à jour, assurez-vous que les microprogrammes de carte réseau sont mis à jour pour corriger l'état d'indisponibilité de DCC, comme recommandé dans l'avis à la clientèle c03600027 (http://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03600027). Pour plus d'informations, reportez-vous à ce Conseil clientèle.

Problèmes connus divers

- **Accès à l'interface CLI refusé après avoir utilisé une clé SSH**

  Après une tentative de connexion à l'interface CLI de Onboard Administrator à l'aide d'une clé SSH, l'accès peut être refusé. Dans ce cas, vous êtes invité à entrer un mot de passe. Ce problème peut se produire avec le mode FIPS activé, après la mise à jour du module Onboard Administrator de la version 3.7x à une version ultérieure. Certains outils utilitaires tiers génèrent des clés inférieures à la longueur minimale autorisée par la version actuelle du module Onboard Administrator. Assurez-vous que la longueur de la clé installée correspond au moins à 2 048 bits. Pour plus d'informations sur les exigences de taille de clé SSH (notamment la taille de type de clé SSH par défaut), consultez le tableau de la section « Fonctionnalités de sécurité cryptographique et valeurs par défaut » (Fonctionnalités de sécurité cryptographique et valeurs par défaut à la page 17).

- **Impossible de se reconnecter au module Onboard Administrator après le réamorçage (Trusted Hosts activé)**

  Avec Trusted Hosts activé, une tentative de reconnexion au module Onboard Administrator à partir d'un client hébergé sur un système d'exploitation qui prend en charge RFC 4941 peut échouer une fois que le système d'exploitation a redémarré.

  RFC 4941 décrit une extension de SLAAC IPv6 qui permet la génération d'adresses IPv6 temporaires au niveau global, à l'aide d'identificateurs d'interface qui changent au fil du temps. Lorsqu'un système d'exploitation qui prend en charge RFC 4941 (tel que Windows 7) est redémarré ou que l'adresse actuelle arrive à expiration, une nouvelle adresse IPv6 temporaire est générée. Lorsque vous accédez au module Onboard Administrator à partir d'un client hébergé sur un système d'exploitation doté d'une prise en charge de RFC 4941, après un réamorçage, la connexion échoue en raison de la nouvelle adresse IPv6 du client et la discordance qui en résulte entre cette adresse et l'adresse IPv6 configurée pour le client dans la liste d'adresses fiables.

  Pour éviter ce problème, désactivez la génération d'adresses IPv6 temporaires de niveau global dans le système d'exploitation ou reconfigurez l'adresse IP approuvée par l'hôte avec l'adresse IPv6 nouvellement générée du client.

- **Échec de génération du certificat (message d'erreur `Could not generate the CSR`)**

  Lorsque vous tentez de générer un certificat à partir du module Onboard Administrator actif ou en Standby, ou que vous utilisez la commande `GENERATE CERTIFICATE`à partir de l'interface CLI, un message d'erreur `Could not generate the CSR` s'affiche. Cela se produit lors d'une tentative de génération d'un certificat auto-signé ou d'une demande de signature de certificat (CSR) et avec les informations obligatoires et facultatives fournies.

  Ce problème peut se produire parce que le nom secondaire facultatif a été spécifié de manière incorrecte. Le nom secondaire doit comprendre entre 0 et 511 caractères, et s'il ne s'agit pas de

0, il doit contenir une liste de paires mot-clé:valeur séparées par des virgules. Les entrées mot-clé-valeur valides incluent IP:<adresse_ip> et DNS:<nom_domaine>.

- **Une tentative d'ajout (téléchargement) d'un certificat utilisateur d'autorité de certification échoue avec une erreur de vérification**

  Lors d'une tentative d'ajout d'un certificat dans l'onglet **Local Users>Administrator>Certificate Information**, le message suivant s'affiche :

  ```
  The user certificate could not be verified. Please upload the
  corresponding CA certificate.
  ```

  Raison et palliatif : Le certificat CA de l'autorité de certification qui a émis ce certificat utilisateur doit être installé à l'aide de l'onglet Certificate Upload de la fonction Two-Factor Authentication.

- **Limitez le nombre de sessions simultanées de support virtuel iLO pour éviter des problèmes de performances et de délai d'expiration**

  Les performances de support virtuel HP c-Class BladeSystem ProLiant et Integrity iLO sont limitées par l'activité et le nombre de sessions simultanées de support virtuel iLO et la charge de travail OA. Les fonctions Enclosure DVD et Enclosure Firmware Management du module Onboard Administrator utilisent la fonction de support virtuel iLO et peuvent avoir des restrictions de performances similaires.

  Pour éviter les problèmes de délai d'attente de support, HP recommande de limiter le nombre de sessions simultanées. Si des problèmes de délai d'attente sont rencontrés lors de l'installation du système d'exploitation ou de mises à jour du microprogramme, réduisez le nombre de sessions de support virtuel en cours, puis redémarrez l'opération.

- **Le lancement du lien Onboard Administrator vers la console distante intégrée iLO 3 peut parfois échouer**

  Le lancement du lien OA vers la console distante intégrée .NET iLO 3 peut parfois échouer. Pour plus d'informations sur la procédure de résolution de ce problème, consultez l'avis à la clientèle c03077476 (http://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03077476).

- **Refus de service pour tentatives de connexion au serveur Web OA**

  Les tentatives de connexion au serveur Web OA sont refusées en raison d'une attaque de refus de service (telle qu'une attaque Slowloris) où un client malveillant ouvre plusieurs connexions TCP pour attacher toutes les connexions disponibles. Pour atténuer les effets des attaques à partir de clients malveillants de serveur Web, vous pouvez utiliser la commande `SET HTTP REQUESTREADTIMEOUT` de l'interface CLI du module Onboard Administrator. Pour plus d'informations, consultez le *Manuel de l'utilisateur de l'interface de ligne de commande HP BladeSystem Onboard Administrator*.

- **Des processus de détection/mise à jour EFM échouent - taille d'image ISO non prise en charge**

  Le module OA prend uniquement en charge les images ISO du SPP qui sont d'une taille inférieure à 4 Go. Si la taille de l'image est de 4 Go ou supérieure, la fonctionnalité EFM échoue. La commande `SHOW FIRMWARE MANAGEMENT` de l'interface CLI OA affiche l'état de l'URL de l'image ISO en tant `Invalid URL`.

  Vous devez créer une image ISO personnalisée qui exclut les composants inutiles pour le processus de mise à jour du microprogramme de lame EFM du module OA. Pour plus d'informations, consultez la section « Enclosure Firmware Management » (Enclosure Firmware Management à la page 195).

- **Après avoir désactivé IPv6 uniquement (passage à un environnement strictement IPv4), EFM ne parvient pas à accéder à l'image ISO**

Après avoir désactivé IPv6 pour configurer un environnement strictement IPv4 (soit par l'intermédiaire de l'onglet **Enclosure Settings > IPv6** ou de la commande d'interface CLI OA `DISABLE IPV6`), si l'URL d'image ISO du microprogramme de l'onglet Enclosure Firmware Management Settings indique un emplacement de clé USB ou une URL basée sur IPv6 pour un serveur Web, l'URL de l'image ISO connue par le module OA continue d'être basée sur IPv6. EFM ne peut pas accéder à l'image ISO en l'état. La solution de contournement consiste à saisir de nouveau l'emplacement de clé USB ou à fournir une URL basée sur IPv4 pour le serveur Web. (Utilisez l'onglet Enclosure Firmware Management Settings de l'interface graphique de OA ou la commande de l'interface CLI OA `SET FIRMWARE MANAGEMENT URL`.)

- **Au cours de la mise à jour de EFM, le message d'erreur « Firmware ISO image is in use, changing URL is not allowed » s'affiche**

  Si, au cours d'une mise à jour de EFM sur une lame de serveur, le serveur est mis hors tension ou la lame de serveur est retirée du boîtier, et que l'utilisateur essaie ensuite de modifier l'URL sur la page EFM de l'interface utilisateur graphique de OA, le message d'erreur « Firmware ISO image is in use, changing URL is not allowed » s'affiche. Il est conseillé de ne pas arrêter ou retirer une lame de serveur pendant l'exécution d'EFM.

- **La page Users/Authentication (LDAP) (Directory Settings) ne se charge pas après une mise à niveau à partir de certaines versions plus anciennes du module OA**

  Après la mise à niveau du module OA en mode FIPS ON/DEBUG à partir de versions antérieures à la version 4.20 ou ultérieure (versions 3.71 à 4.11), la page **Users/ Authentication>Directory Settings** ne se charge pas. Le message suivant s'affiche :

  ```
  The key strength for the provided key is invalid for this
  configuration. (La puissance de la clé fournie n'est pas valide pour
  cette configuration.)
  ```

  Cela résulte des fonctions de sécurité plus robustes mises en œuvre à compter de OA 4.20. La longueur minimum de clé a été augmentée à 2 048 bits. Le message d'erreur indique que le module OA a détecté des certificats LDAP contenant des clés non conformes qui avaient été installés sur la version antérieure du module OA.

  L'administrateur OA doit retirer les clés non conformes et les remplacer par des clés de 2 048 bits ou plus.

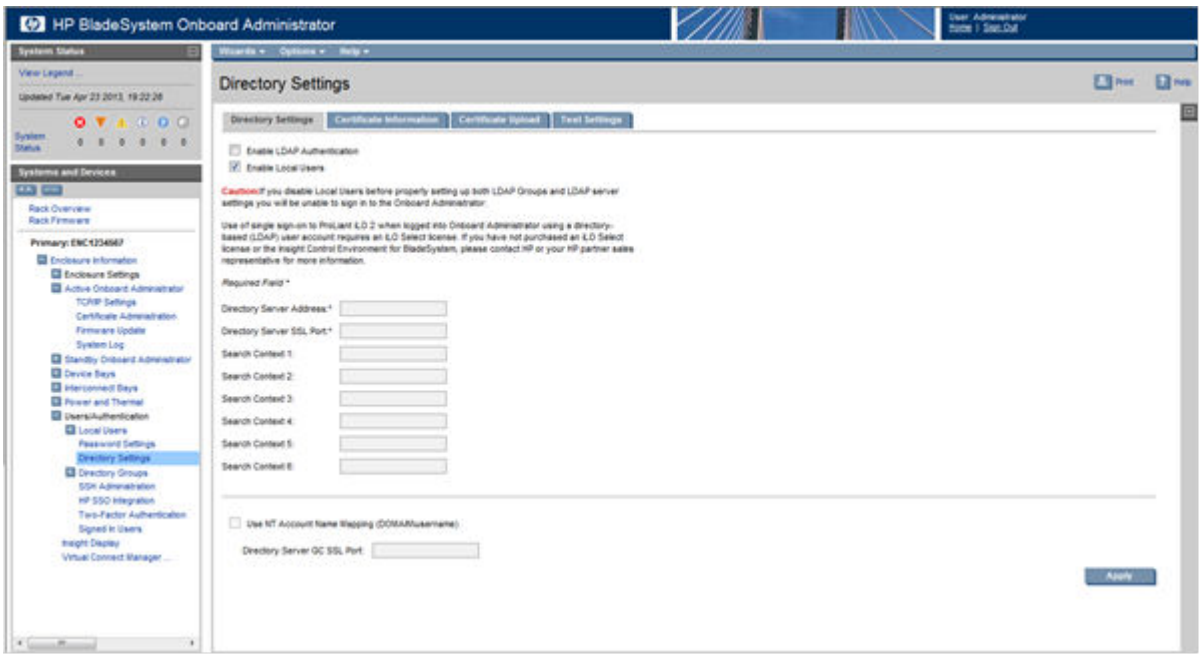
12 Activation de l'authentification de services d'annuaire LDAP auprès de Microsoft Active Directory

Services de certificat

La mise en œuvre Microsoft® de LDAP via SSL requiert que le contrôleur de domaine installe un certificat DC provenant de l'autorité de certification (CA) de l'organisation. Ce processus se produit lorsque le service Enterprise Root CA est ajouté à un serveur dans Active Directory. HP recommande fortement d'utiliser le service Enterprise Root CA pour minimiser les complexités de demande et d'acceptation de certificats de contrôleur de domaine auprès d'une CA autonome.

REMARQUE : La fonction LDAP du module Onboard Administrator prend en charge Microsoft® Active Directory à l'aide de l'attribut `memberOf`. Novell eDirectory est également pris en charge avec l'attribut `groupMembership`. OpenLDAP n'est pas pris en charge.

Préparation de l'annuaire



Pour préparer l'annuaire :

1. Créez un groupe Active Directory nommé OA Admins, puis ajoutez un utilisateur nommé TestAdmin dans ce groupe.
2. Créez un groupe nommé OA Operators, puis ajoutez un utilisateur nommé TestOperator dans ce groupe. Peu importe les autorisations utilisateur.

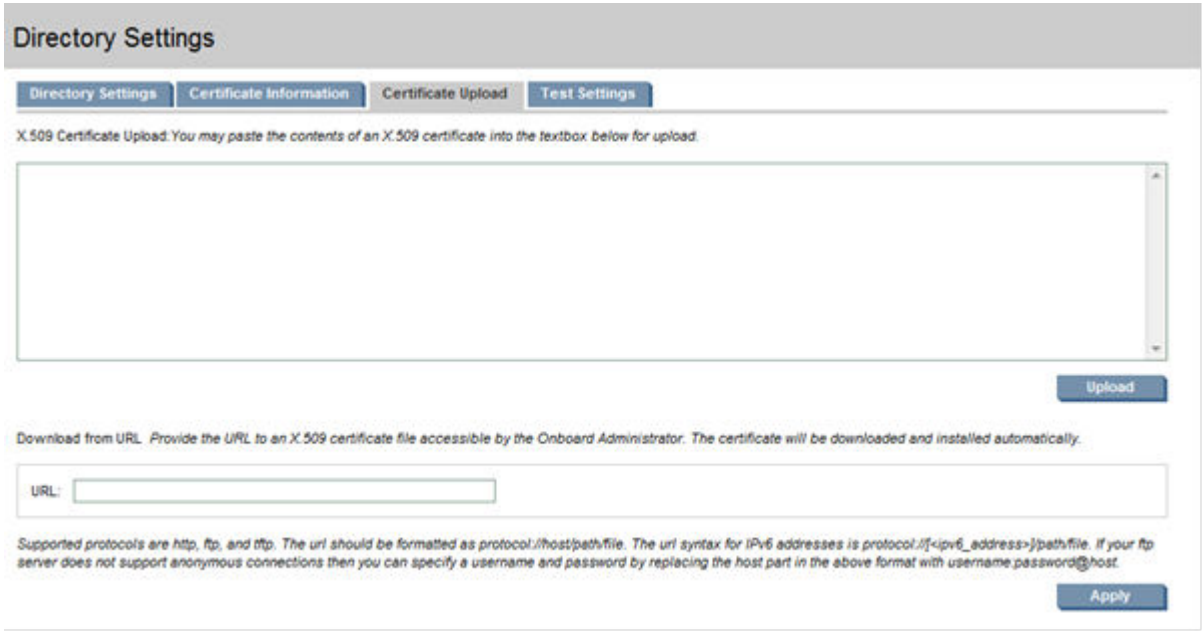
3. Naviguez vers l'écran Directory Settings (Paramètres d'annuaire) situé sous Users/Authentications (Utilisateurs/Authentifications) pour le boîtier souhaité.
4. Cliquez sur **Enable LDAP** (Activer LDAP), puis entrez l'adresse IP ou le nom d'un de vos contrôleurs de domaine. Pour plus d'informations sur la vérification si le contrôleur de domaine écoute sur le port 636, consultez la section « Résolution des problèmes LDAP sur Onboard Administrator » (Résolution des problèmes LDAP sur Onboard Administrator à la page 402). Sinon, pour forcer les serveurs DNS définis pour le domaine à offrir des contrôleurs de domaine, entrez le nom de domaine de votre domaine AD (DOMAIN.COM) au lieu d'un nom de serveur. Pour plus de simplicité au cours de la configuration initiale, HP recommande d'utiliser une adresse IP unique. Le contexte de recherche est au format LDAP standard. Par exemple, si les comptes utilisateur sont dans l'unité organisationnelle Users dans un domaine nommé BLADEDEMO.HP.COM, le contexte de recherche sera :

   CN=Users,DC=bladedemo,DC=hp,DC=com

Téléchargement du certificat de contrôleur de domaine (facultatif)

Vous pouvez télécharger plusieurs certificats de contrôleur de domaine. Téléchargez un certificat qui autorise LDAP via SSL.

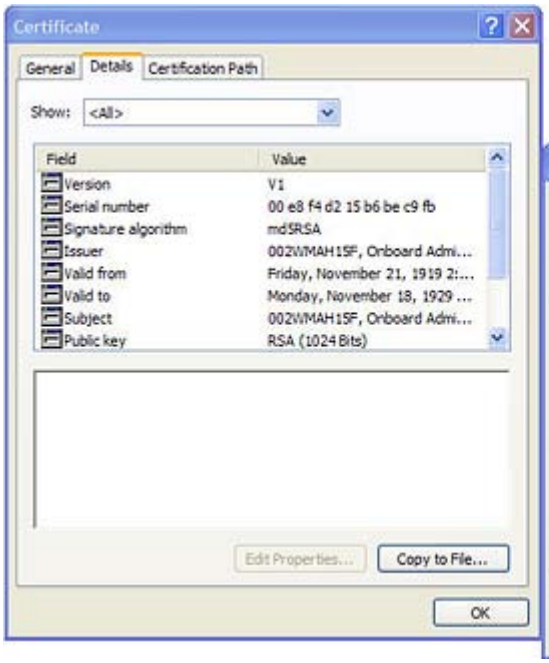
1. Cliquez sur l'onglet **Upload Certificate** (Télécharger un certificat).


Directory Settings
Directory Settings
Certificate Information
Certificate Upload
Test Settings
X.509 Certificate Upload You may paste the contents of an X.509 certificate into the textbox below for upload.
Upload
Download from URL. Provide the URL to an X.509 certificate file accessible by the Onboard Administrator. The certificate will be downloaded and installed automatically.
URL:
Supported protocols are http, ftp, and tftp. The url should be formatted as protocol://host/path/file. The url syntax for IPv6 addresses is protocol://[<ipv6_address>]/path/file. If your ftp server does not support anonymous connections then you can specify a username and password by replacing the host part in the above format with username:password@host.
Apply

2. Obtenez le certificat du DC en ouvrant une nouvelle fenêtre de navigateur Web à l'adresse https://<*contrôleur_domaine*>:636 (où *contrôleur_domaine* est votre DC). Cette URL HTTPS étant sécurisée, vous êtes donc invité à accepter un certificat. Cliquez sur **View Certificate** (Afficher le certificat).

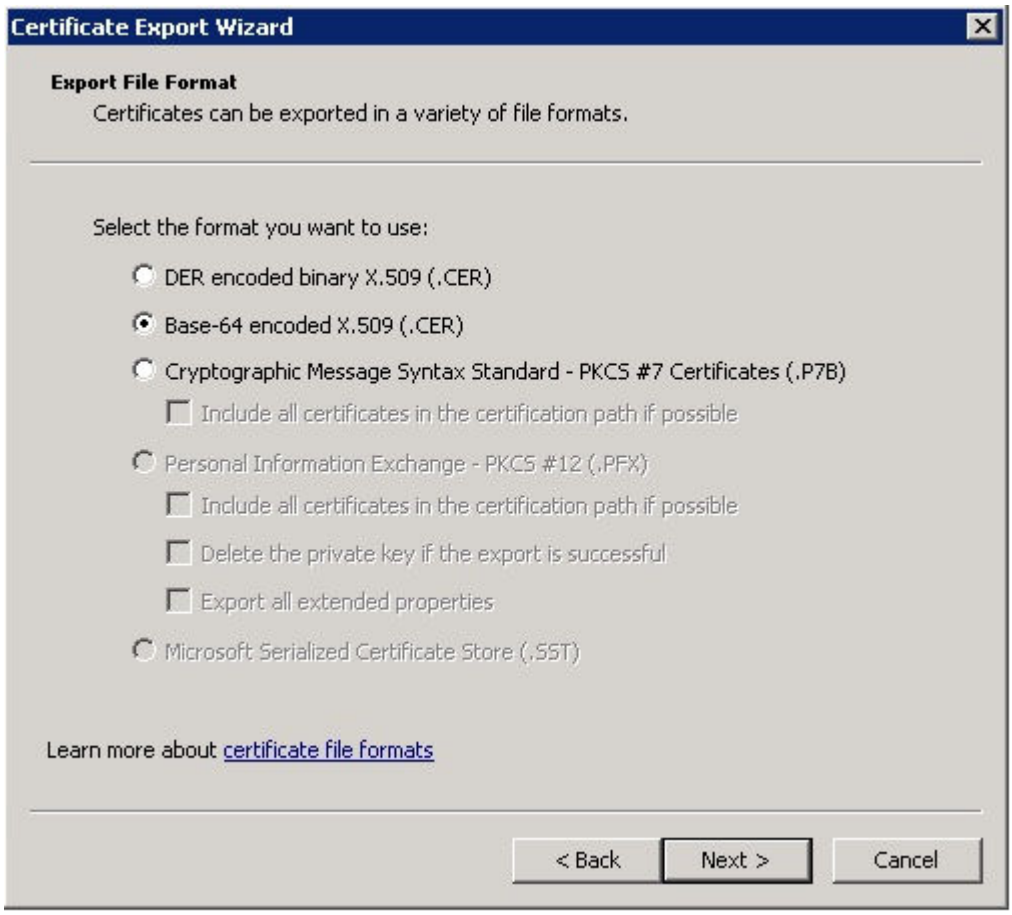
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate has expired or is not yet valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

3. Cliquez sur l'onglet **Details** (Détails), puis sur **Copy to File** (Copier dans fichier).



Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

4. Sélectionnez **Base-64 encoded x.509 (.CER)** dans la liste des options d'exportation (ceci est important). Fournissez un nom et un emplacement pour le fichier (c:\dccert.cer), puis terminez l'exécution de l'assistant.


Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Microsoft Serialized Certificate Store (.SST)
Learn more about certificate file formats
< Back
Next >
Cancel

5. Repérez le fichier de certificat exporté et renommez-le avec une extension .txt (par exemple, dccert.txt). Ouvrez le fichier dans un éditeur de texte, puis copiez le contenu entier vers le Presse-papiers. Voici un exemple du contenu du fichier de certificat :

```
-----BEGIN CERTIFICATE-----
MIIFxDCCBKygAwIBAgIKJWUSwAAAAAAAAjANBgkqhkiG9w0BAQUFADBVMRMwEQYK
CZImiZPyLGQBGRYDY29tMRIwEAYKCZImiZPyLGQBGRYCaHAxFzAVBgoJkiaJk/Is
ZAEZFgdhdGxkZW1vMREwDwYDVQQDEwh3aW5kb3pDQTAeFw0wNjA4MjIyMDIzMTFa
Fw0wNzA4MjIyMDIzMTFaMCAxHjAcBgNVBAMTFXdpbmRvei5hdGxkZW1vLmhwLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAy4zeh3iXydUAWKVHIDsxLJ6B
aRuVT9ZhkL5NQHIDeRjumsgc/jHSERDmHuyoY/qbF7JMhJ9Lh9QQHUg8QfEYsC1y
qTvgisrZeHtvmrmecvSxZm27b4Bj5XYN0VYcrwqKnH7X/tVhmwqGls7/YZyahNU1
lGB2OjoCq5eJxX+Ybx0CAwEAAaOCA00wggNJMAsGA1UdDwQEAwIFoDBEBgkqhkiG
9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4D
…output truncated…
```

```
-----END CERTIFICATE-----
```

6. Revenez à l'écran OA Upload Certificate, collez le contenu du certificat dans la fenêtre, puis cliquez sur **Upload** (Charger).

Création de groupes d'annuaire

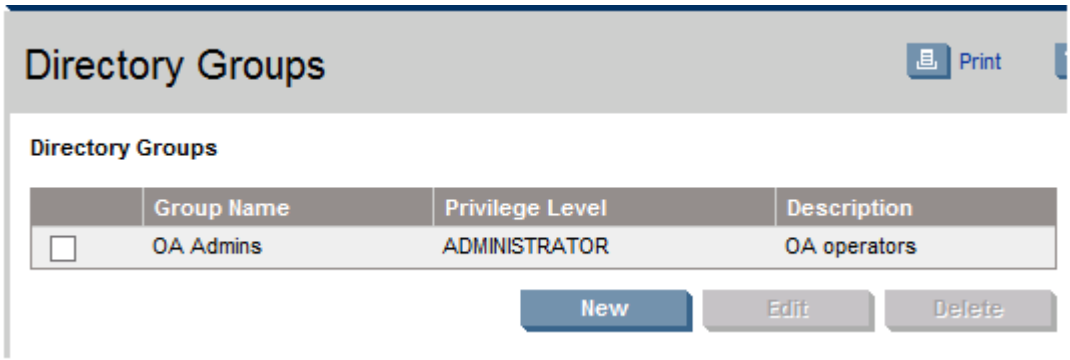
Le module Onboard Administrator authentifie les utilisateurs et attribue des privilèges en vérifiant au préalable que le nom d'utilisateur et le mot de passe fournis correspondent aux informations de connexion dans l'annuaire. Une fois une correspondance vérifiée, le module Onboard Administrator interroge l'annuaire pour connaître les noms des groupes Active Directory auxquels appartient l'utilisateur. Le module Onboard Administrator contrôle ensuite ces noms de groupe par rapport aux noms de groupe d'annuaires existant dans le module Onboard Administrator. Dans l'exemple suivant, des groupes d'annuaires Onboard Administrator sont créés dans cette étape. Le nom de groupe est utilisé pour déterminer l'appartenance du groupe d'utilisateurs LDAP et doit correspondre à l'une des cinq propriétés suivantes d'un groupe d'annuaires : le nom, le nom unique, le nom commun, le nom d'affichage ou le nom de compte SAM.

Pour créer un groupe d'annuaires :

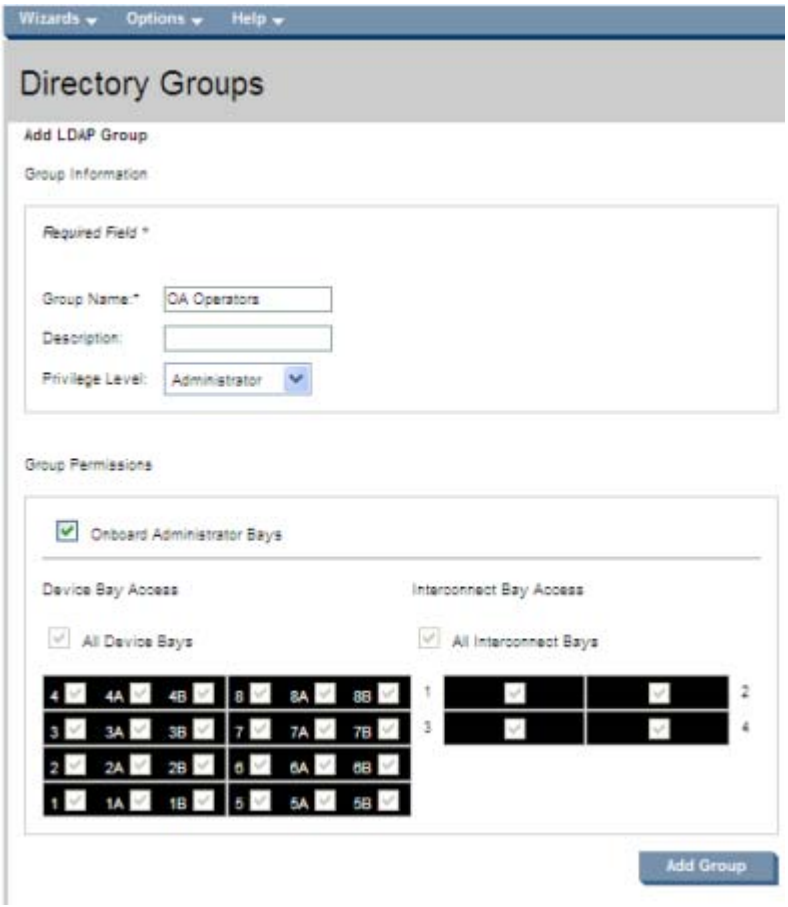
1. Dans le module Onboard Administrator, naviguez vers le lien **Users>Authentications>Directory Groups** (Utilisateurs>Authentifications>Groupes d'annuaires).
2. Pour ajouter un nouveau groupe d'annuaires, cliquez sur **New** (Nouveau).
3. Créez un groupe nommé OA Admins, qui est le même nom que celui créé dans Active Directory.

REMARQUE : Les noms de groupe avec des espaces peuvent ne pas être pris en charge sur certains serveurs LDAP.

4. Attribuez à ce groupe des privilèges d'administration complets sur toutes les baies de serveur et baies d'interconnexion, puis cliquez sur **Add** (Ajouter).



5. Créez un deuxième groupe d'annuaires nommé OA Operators correspondant au groupe d'opérateurs créés dans Active Directory. Cette fois, attribuez le privilège Operator (Opérateur) au groupe au lieu d'Administrator (Administrateur), et n'accordez pas au groupe l'accès aux baies de serveur, mais autorisez l'accès aux baies d'interconnexion, puis cliquez sur **Add** (Ajouter).



Si vous rétrogradez le microprogramme Onboard Administrator de la version 2.40 à la version 2.31, vous perdez tous les groupes en plus des cinq premiers groupes. Le microprogramme Onboard Administrator version 2.40 prend en charge 20 groupes, alors que les versions antérieures prennent uniquement en charge cinq groupes.

Test de la solution de connexion à l'annuaire

1. Déconnectez-vous de la session Onboard Administrator actuelle, puis fermez toutes les fenêtres de navigateur.
2. Naviguez vers le module Onboard Administrator, puis connectez-vous en utilisant une des options suivantes :
   - TestAdmin
   - TestAdmin@domain.com
   - DOMAIN\TestAdmin
   - FQDN: cn=<TestAdmin>,cn=<users>dc=<domain>,dc=<com>

3. Entrez le mot de passe correspondant utilisé pour le compte utilisateur. Si vous ne pouvez pas vous connecter avec des privilèges d'administration complets, consultez la section « Résolution des problèmes LDAP sur Onboard Administrator » (Résolution des problèmes LDAP sur Onboard Administrator à la page 402). Notez que vous ne pouvez pas vous connecter en utilisant votre nom d'utilisateur. Par exemple, si votre nom de compte est John Brownie et que votre compte est jbrownie, vous ne pouvez pas vous connecter en tant que jbrownie car ce format n'est pas actuellement pris en charge par LDAP.
4. Déconnectez-vous du module Onboard Administrator, puis connectez-vous en utilisant une des options suivantes :
   - TestOperator
   - TestOperator@Domain.com
   - DOMAIN\TestOperator
   - FQDN: cn=<TestOperator>,cn=<users>dc=<domain>,dc=<com>
5. Entrez le mot de passe correspondant utilisé pour ce compte. Vous avez un accès intégral aux baies d'interconnexion mais à aucune lame de serveur.

Résolution des problèmes LDAP sur Onboard Administrator

Pour vérifier que SSL fonctionne sur les contrôleurs de domaine dans votre domaine, ouvrez un navigateur et naviguez vers l'adresse https://*<contrôleur_domaine>*:636 (où <contrôleur_domaine> est votre contrôleur de domaine). Vous pouvez remplacer <contrôleur_domaine> par <domaine>, qui accède au DNS afin de vérifier quel contrôleur de domaine traite actuellement les demandes pour le domaine. Testez plusieurs contrôleurs de domaine afin de vérifier que chacun a reçu un certificat. Si SSL fonctionne correctement sur un contrôleur de domaine (signifiant par exemple qu'un certificat a été émis pour celui-ci), une boîte de dialogue de sécurité permet de choisir entre accéder au site ou visualiser le certificat du serveur. Si vous cliquez sur Yes (Oui), aucune page Web ne s'affiche. L'objet du test est de générer une invite pour accepter la boîte de dialogue de sécurité. Un serveur qui n'écoute pas sur le port 636 produit un message « `La page ne peut pas être affichée` ». Si ce test échoue, cela signifie que le contrôleur de domaine n'accepte pas les connexions SSL, probablement parce qu'aucun certificat n'a été émis. Ce processus est automatique, mais peut requérir un redémarrage.

Pour éviter un redémarrage :

1. Sur le contrôleur de domaine, chargez le module enfichable MMC « Computer Account » (Compte d'ordinateur), puis naviguez vers le dossier Personal->Certificates (Personnel->Certificats).
2. Cliquez avec le bouton droit sur le dossier, puis sélectionnez **Request New Certificate** (Demander nouveau certificat). Le type par défaut est « Domain Controller » (Contrôleur de domaine).
3. Cliquez sur **Next** (Suivant), puis répétez la procédure jusqu'à ce que le contrôleur de domaine émette le certificat.

Une deuxième méthode de résolution des problèmes SSL consiste à accéder au contrôleur de domaine et à exécuter la commande suivante :

```
C:\netstat -an | find /i "636"
```

Si le serveur écoute les demandes sur le port 636, la réponse suivante s'affiche :

```
 TCP 0.0.0.0:636 0.0.0.0:0 LISTENING
```

1. Un troisième problème peut être dû au fait que les contrôleurs de domaine n'ont pas été enregistrés automatiquement. L'auto-enregistrement et l'émission des certificats des contrôleurs de domaine peuvent prendre jusqu'à huit heures car Microsoft utilise GPO pour avertir les contrôleurs de domaine de l'autorité de certification nouvellement installée. Vous pouvez forcer ceci en exécutant DSSTORE -pulse à partir des contrôleurs de domaine (outil disponible dans le kit de ressources w2k). Ce processus étant déclenché par winlogon. Ainsi, pour que l'enregistrement automatique fonctionne, vous devez vous déconnecter, puis vous reconnecter. Les certificats apparaissent automatiquement dans la liste des certificats émis par les autorités de certification. Assurez-vous que l'autorité de certification ne les répertorie pas dans la liste de certificats en attente. Si tel est le cas, modifiez l'autorité de certification pour émettre automatiquement des certificats lorsqu'une demande est présentée. Si la fonction d'inscription automatique ne fonctionne toujours pas, demandez le certificat à l'aide de la procédure suivante :
2. Sur le contrôleur de domaine, ouvrez MMC, puis ajoutez le module enfichable de certificats (Compte d'ordinateur).
3. Naviguez vers Personal, puis cliquez avec le bouton droit sur le dossier.
4. Cliquez sur **Request New Cert** (Demander nouveau certificat), puis sur **Next** (Suivant).
5. Entrez un nom pour le certificat.

Si une erreur RPC se produit, vérifiez que l'autorité de certification est répertoriée dans DNS et qu'elle est exécutée.

Si l'assistant ne démarre pas, forcez le serveur pour afficher l'autorité de certification et permettre l'exécution de l'assistant :

Pour accélérer le processus GPO et permettre aux contrôleurs de domaine de reconnaître l'autorité de certification, utilisez une des commandes suivantes :

- Windows® 2003, Gpupdate /force
- Windows® 2000, Secedit /refreshpolicy machine_policy /enforce

Vérifiez que le module Onboard Administrator dispose de tous les paramètres réseau appropriés (tels que DNS) et que les date et heure sont correctes (les certificats respectent l'heure). Assurez-vous que le module Onboard Administrator peut atteindre le serveur DNS (envoyez-lui une commande ping à partir de l'interface de ligne de commande Onboard Administrator).

Si LDAP est activé lors du démarrage en mode Mot de passe perdu, le mot de passe Administrateur local est réinitialisé, LDAP est désactivé et la connexion locale est réactivée.

REMARQUE : La fonction LDAP du module Onboard Administrator prend en charge Microsoft® Active Directory à l'aide de l'attribut `memberOf`. Novell eDirectory est également pris en charge avec l'attribut `groupMembership`. OpenLDAP n'est pas pris en charge.

13 Création d'autorités de certification et configuration de l'autorisation à deux facteurs pour comptes de groupe LDAP et d'utilisateur local

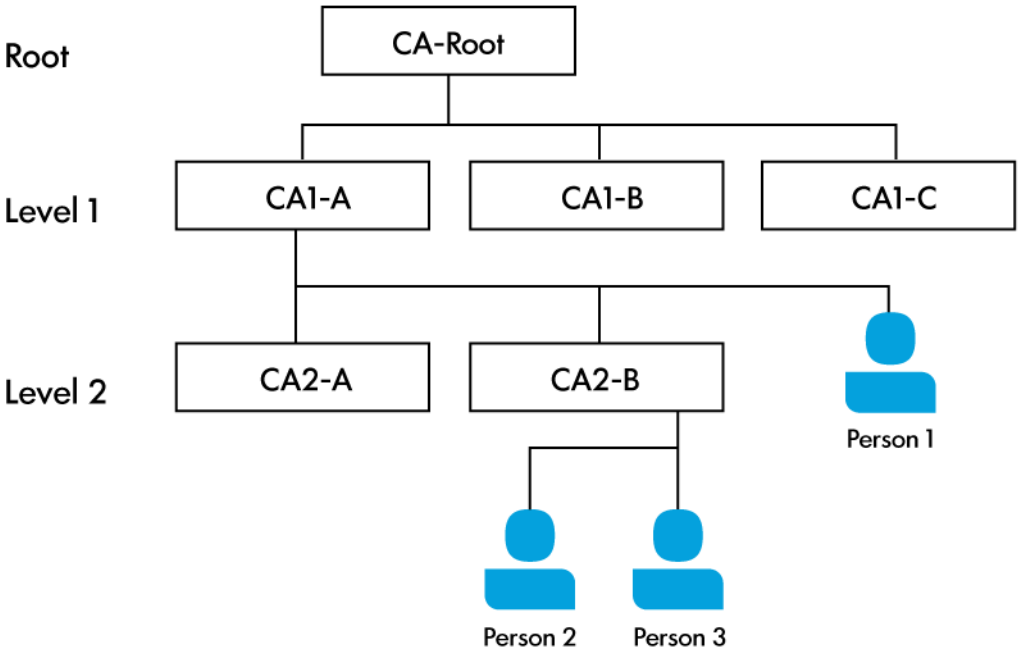
Introduction

L'authentification à deux facteurs est une fonctionnalité facultative qui fournit une sécurité améliorée pour le module Onboard Administrator. Pour autoriser l'accès au module Onboard Administrator, l'authentification à deux facteurs requiert quelque chose que l'utilisateur a (un certificat) et quelque chose qu'un utilisateur connaît (un mot de passe ou code PIN). Le certificat est stocké directement dans un navigateur ou sur le périphérique d'accès (comme une carte à puce, un dongle ou un module TPM).

Vous pouvez utiliser l'authentification à deux facteurs avec des comptes d'utilisateur local ou des comptes de groupe d'annuaire (LDAP). Pour les comptes LDAP, vous pouvez utiliser l'objet ou l'autre nom d'objet pour fournir le nom de connexion LDAP. Dans tous les cas, le certificat utilisateur doit être validé par rapport à une autorité de certification.

Mappage de l'infrastructure à clé publique de l'authentification à deux facteurs

Les autorités de certification sont basées sur une structure d'arborescence. Les certificats racine sont auto-signés. Il est possible de remonter à la racine de tous les autres certificats en suivant le champ d'émetteur du certificat. Les certificats utilisateur peuvent être publiés par n'importe laquelle des autorités de certification dans l'arborescence. Le module Onboard Administrator dispose d'un espace de stockage limité et par conséquent prend en charge un maximum de 12 certificats CA. Le schéma suivant illustre une structure d'arborescence similaire à celle utilisée dans les exemples à suivre.



Les mappages d'autorité de certification peuvent être très simples ou complexes. Pour un exemple de mappage complexe, reportez-vous à l'infrastructure à clé publique du Ministère de la défense des États-Unis (http://iase.disa.mil/pki-pke/interoperability/).

Étapes de création d'autorités de certification et configuration de l'authentification à deux facteurs avec comptes de groupe LDAP et d'utilisateur local

Les sections suivantes fournissent des instructions et exemples de création d'autorités de certification et de configuration de l'authentification à deux facteurs avec comptes de groupe LDAP et d'utilisateur local. Dans un but de simplicité, les certificats d'autorité de certification dans les exemples fournis sont créés sur un système unique au lieu de plusieurs systèmes. Une mise en œuvre réelle des autorités de certification utiliserait plusieurs systèmes.

Le tableau suivant répertorie les étapes de configuration de l'authentification à deux facteurs avec des comptes de groupe LDAP et d'utilisateur local, et indique la section documentant chaque étape ainsi que toutes les étapes subordonnées.

Étape	Section
1	Configuration des répertoires (Configuration des répertoires à la page 407) • Création des répertoires initiaux pour l'autorité de certification racine • Modification et stockage d'un fichier de configuration OpenSSL dans chaque autorité de certification • Modification des répertoires par défaut pour répondre aux besoins de votre structure
2	Création d'une autorité de certification racine (Création d'une autorité de certification racine à la page 408) • Copie du fichier de configuration OpenSSL vers l'autorité de certification racine • Création du certificat d'autorité de certification racine et de clé privée • Création d'une combinaison de fichier PEM de certificat et de clé privée d'autorité de certification racine

Étape	Section
3	Création d'autorités de certification subordonnées (Création d'autorités de certification subordonnées à la page 410) • Création des répertoires pour les autorités de certification subordonnées • Fourniture d'informations de certificat x509 • Génération d'une clé de serveur et d'une CSR pour chaque autorité de certification subordonnée • Signature de la CSR par l'autorité de certification racine
4	Création de clés d'utilisateur et de CSR (Création de clés d'utilisateur et de CSR à la page 412) • Création des répertoires pour les clés d'utilisateur et CSR • Fourniture d'informations de certificat x509 • Génération d'une clé de serveur et d'une CSR pour chaque utilisateur • Signature de la CSR par l'autorité de certification subordonnée appropriée
5	Vérification de certificats (Vérification de certificats à la page 416)
6	Stockage d'un certificat utilisateur sur une carte à puce ou un navigateur
7	Configuration du module Onboard Administrator pour l'authentification à deux facteurs avec comptes locaux (Configuration du module Onboard Administrator pour l'authentification à deux facteurs avec comptes locaux à la page 419) • Établissement d'un plan de récupération de module Onboard Administrator • Configuration du délai d'expiration de session Onboard Administrator • Installation de la chaîne d'autorités de certification • Installation de certificats utilisateur sur le compte administrateur local • Activation de l'authentification à deux facteurs • Connexion au module Onboard Administrator à l'aide de l'authentification à deux facteurs
8	Activation de l'authentification TFA+LDAP (Activation de l'authentification TFA+LDAP à la page 428)

Les sections suivantes incluent également :

- Méthodes de spécification du champ d'objet sur une CSR (Méthodes de spécification du champ d'objet sur une CSR à la page 428)
- Résolution des problèmes d'authentification TFA et LDAP (Résolution des problèmes d'authentification TFA et LDAP à la page 429)
- Exemples de l'interface CLI pour configuration d'un compte utilisateur et de certificats (Exemples de l'interface CLI pour configuration d'un compte utilisateur et de certificats à la page 430)
- Informations sur les autorités de certification et les certificats disponibles à partir du Web (Informations sur les autorités de certification et les certificats disponibles à partir du Web à la page 432)

Configuration des répertoires

Cette section décrit les étapes de configuration requises avant de créer l'autorité de certification racine.

Création d'un répertoire pour représenter chaque autorité de certification et chaque utilisateur

Dans ce didacticiel, l'exemple suivant configure les répertoires initiaux pour l'autorité de certification racine. Une description de chaque répertoire suit. Dans cet exemple et les suivants, l'entrée utilisateur aux invites est indiquée par une saisie en **caractères gras**.

REMARQUE : Il s'agit d'un didacticiel pour la création d'autorités de certification dans un environnement de test simple. Dans un environnement de production réel, les serveurs d'autorités de certification seraient sur des serveurs distincts. Dans cet exemple didactique, les serveurs d'autorités de certification sont représentés par des répertoires distincts sur un serveur unique.

```
[~/]$ mkdir -m 0755 ~/examples
[~/]$ mkdir -m 0755 \
 ~/examples/rootCA \
 ~/examples/rootCA/private \
 ~/examples/rootCA/certs \
 ~/examples/rootCA/newcerts \
 ~/examples/rootCA/crl
[~/]$ mkdir -m 0755 \
 ~/examples/level1CA \
 ~/examples/level1CA/private \
 ~/examples/level1CA/certs \
 ~/examples/level1CA/newcerts \
 ~/examples/level1CA/crl
[~/]$ mkdir -m 0755 \
 ~/examples/TestUser \
 ~/examples/TestUser/private \
 ~/examples/TestUser/certs
```

Description des répertoires

- `./private` : l'emplacement des clés privées. Normalement, les autorisations sur ce répertoire devraient être configurées pour limiter l'accès en lecture à la racine (0200) ou au compte utilisateur pour le serveur Web. Cet exemple démarre avec un accès en lecture/écriture complet pour tout le monde (0755).
- `./certs` : l'emplacement des certificats d'autorité de certification.

- `./newcerts` : l'emplacement des nouveaux certificats signés. Ils sont stockés dans un format PEM non crypté avec un format de nom de fichier *cert_serial_number.pem* (tel que `03.pem`).
- `./crl` : l'emplacement de la liste de révocation des certificats.

Modification et stockage d'un fichier de configuration OpenSSL dans chaque répertoire d'autorité de certification

Le fichier de configuration OpenSSL (`openssl.cnf`) contient la structure de répertoires par défaut, les noms et les options. Sur la plupart des distributions Linux, un fichier `openssl.cnf` par défaut est situé dans `/etc/pki/tls`, comme illustré dans l'exemple suivant.

```
[~/examples]$ cp -v /etc/pki/tls/openssl.cnf ~/examples/
```

Modification des répertoires par défaut

Dans cet exemple, une modification est apportée pour l'ensemble des autorités et des utilisateurs. Vous pouvez utiliser ce fichier comme modèle pour les autres répertoires.

```
####################################################################

[ CA_default ]

dir = . # CHANGE from "../../CA" # Everything is stored here

certs = $dir/certs # Issued certs are stored here
```

Création d'une autorité de certification racine

Cette section décrit les étapes pour la création d'une autorité de certification racine.

Copie du fichier de configuration OpenSSL dans le répertoire de l'autorité de certification racine

Copiez le fichier `openssl.cnf` dans le répertoire de l'autorité de certification racine (`rootCA` dans cet exemple) :

```
[~/examples]$ cp ~/examples/openssl.cnf ~/examples/rootCA/openssl-rootCA.cnf

[~/examples]$ cd ~/examples/rootCA
```

Création du certificat et de la clé privée

Créez la clé de l'autorité de certification racine et un certificat (`rootCA-private.key` et `rootCA.crt`). Dans l'exemple suivant, la longueur de clé est définie sur 2048 et l'algorithme de signature de hachage sur SHA256. Lorsque vous y êtes invité, entrez une phrase secrète de sécurité. Lors de l'utilisation de l'option `-nodes`, vous pouvez omettre la phrase secrète. Lorsque vous êtes invité à entrer des paramètres tels que pays, état, ville et ainsi de suite, vous pouvez spécifier un champ vide en entrant un point ("."), comme indiqué.

```
[~/examples/ rootCA]$ openssl req -config ./openssl-rootCA.cnf -newkey
\rsa:2048 -x509 -extensions v3_ca -keyout private/rootCA-private.key -out
\certs/rootCA.crt -days 1825 -sha256 -nodes

Generating a 2048 bit RSA private key

.................+++
```

```
.............+++
writing new private key to 'private/rootCA-private.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]: .
State or Province Name (full name) [Berkshire]: .
Locality Name (eg, city) [Newbury]: .
Organization Name (eg, company) [My Company Ltd]: .
Organizational Unit Name (eg, section) []: .
Common Name (eg, your name or your server's hostname) []: My Root CA
Email Address []: .

[~/examples/rootCA]$ ]$ ls -l private/ certs/
certs/:
total 4
-rw-rw-r-- 1 xxx 1314 Nov 10 08:11 rootCA.crt

private/:
total 4
-rw-rw-r-- 1 xxx 1675 Nov 10 08:11 rootCA-private.key
```

Pour vérifier que le certificat nouvellement créé est correct, affichez le certificat en entrant la commande illustrée dans l'exemple suivant :

```
[~/examples/rootCA]$ openssl x509 -in certs/rootCA.crt -text
```

Pour un certificat racine auto-signé, les champs `-issuer` et `-subject` doivent correspondre. Pour vérifier qu'ils correspondent, utilisez la commande suivante pour afficher uniquement les champs `-issuer` et `-subject` :

```
[~/examples/rootCA]$ openssl x509 -in certs/rootCA.crt \
 -noout -issuer -subject
```

Création d'un fichier PEM combiné de certificat et de clé privée

Un fichier PEM combiné de certificat et de clé privée est nécessaire lorsque l'autorité de certification contre-signe d'autres certificats. Le fichier est référencé par le fichier de configuration OpenSSL. Les commandes suivantes modifient le répertoire par défaut et créent le fichier PEM combiné de certificat et de clé privée `cakey.pem` :

```
[ ]$ cd ~/examples/rootCA

[ rootCA]$ cat private/rootCA-private.key certs/rootCA.crt > private/
cakey.pem
```

Création d'autorités de certification subordonnées

Cette section décrit les étapes pour la création de certificats de serveur qui sont émis (signés) par une autre autorité de certification.

Création de répertoires pour l'autorité de certification subordonnée

Si elle n'est pas déjà présente, créez la structure de répertoires pour contenir la base de données de l'autorité de certification subordonnée, comme indiqué dans l'exemple suivant :

```
[~/]$ mkdir -m 0755 \
 ~/examples/level1CA \
 ~/examples/level1CA/private \
 ~/examples/level1CA/certs \
 ~/examples/level1CA/newcerts \
 ~/examples/level1CA/crl
```

Copiez le fichier `openssl.cnf` modifié dans le répertoire de travail, comme indiqué :

```
[~/examples]$ cp -v openssl.cnf level1CA/

`openssl.cnf' -> `level1CA/openssl.cnf'
```

Fourniture d'informations de certificat x509

Un certificat comprend un grand nombre d'éléments de données qui décrivent le certificat. Les données peuvent être entrées manuellement lorsque vous y êtes invité ou fournies automatiquement via un fichier de configuration OpenSSL. La sortie suivante illustre un exemple sur la façon de créer un fichier de configuration OpenSSL via un fichier de script.

```
#!/bin/sh

#

cat << _end_marker_ > openssl-level1CA.cnf

[ req ]

distinguished_name=req_DN

attributes=req_attr

prompt=no
```

```
[ req_DN ]
CN=level1CA
C=US
ST=TX
L=Houston
O=Development
subjectAltName=otherName:Gorilla
OU=Jungle
emailAddress=george@theJungle.com
surname=.
givenName=Frederick
initials=FGG
# dnQualifier=
name=George of the Jungle

[ req_attr ]
# challengePassword=
# unstructuredName=

_end_marker_
```

Génération d'une CSR et d'une nouvelle clé de serveur

Cette étape génère une nouvelle clé (`-newkey`) et génère une CSR qui peut être soumise à une autorité de certification. La nouvelle clé privée est stockée dans l'emplacement `keyout`. La CSR est vidée dans le paramètre `-out`. Pour plus de simplicité, l'option `-nodes` est utilisée pour éliminer la nécessité d'une protection à partir d'une phrase secrète.

```
[~/examples/level1CA]$ openssl req -config ./openssl-level1CA.cnf -newkey rsa:2048 -sha256 -keyout \ ./private/level1CA-private.key -nodes -out ./temp-level1CA.csr
```

Génération d'une CSR sans génération d'une nouvelle clé (facultatif)

Générez la CSR sans générer une nouvelle clé privée, comme dans cet exemple :

```
[~/examples/level1-ca]$ openssl req -config ./openssl-level-1-ca.cnf \
-new -key ./level-1-CA-private.key -nodes -out ./level-1-CA.csr
```

Affichage de la clé privée

Pour afficher la clé privée, utilisez la commande illustrée dans l'exemple suivant :

```
[~/examples/level1CA]$ openssl rsa -in ./private/level1CA-private.key -text
```

Signature de la CSR level1CA avec la clé rootCA

Une fois une CSR générée (à l'étape précédente), elle doit être signée par une autorité de certification établie dans la chaîne de confiance. Après la première demande de signature (lorsque seule existe l'autorité de certification racine), la CSR doit être signée par l'autorité de certification racine. Les CSR ultérieures peuvent être signées par des autorités de niveau inférieur, si elles ont une autorisation à le faire.

Dans cet exemple, l'autorité de certification racine signe la CSR de premier niveau (`level-1-CA.csr`).

1. Accédez à l'autorité de certification qui va effectuer la signature, puis affichez la CSR et vérifiez qu'il s'agit de celle que vous souhaitez vraiment signer :

   ```
   [ ]$ cd ~/examples/rootCA/

   [ rootCA]$ openssl req -in ../level1CA/temp-level1CA.csr -noout -text
   ```

2. Effectuez l'étape suivante de la configuration ponctuelle :

   ```
   [ rootCA]$ echo '01' > serial

   [ rootCA]$ touch index.txt
   ```

3. Après avoir vérifié que vous souhaitez signer la CSR, obtenez la signature de la CSR en exécutant la commande suivante :

   ```
   [~/examples/rootCA]$ openssl ca \
    -config openssl-rootCA.cnf \
    -extensions v3_ca -policy policy_anything \
    -in ../level1CA/temp-level1CA.csr \
    -cert certs/rootCA.crt \
    -default_md sha256 \
    -key private/rootCA-private.key
   ```

   Le certificat signé est écrit dans `./certs/{`*serialNumber*`}.pem`. Les fichiers `serial` et `index.txt` ont été mis à jour.

4. Installez le certificat sur le serveur d'autorité de certification de premier niveau, en spécifiant le numéro de série approprié (dans cet exemple, le numéro de série est `01`).

   ```
   [ ~]$ cp ~/examples/rootCA/newcerts/01.pem ~/examples/level1CA/certs/
   level1CA.pem
   ```

Création de clés d'utilisateur et de CSR

Les étapes pour la création d'une nouvelle clé d'utilisateur et d'une CSR sont similaires à celles pour la création d'une CSR pour une autorité de certification à l'exception près qu'un type différent est spécifié.

Création d'un répertoire pour la clé utilisateur et la base de données de CSR

Si elle n'est pas déjà présente, créez la structure de répertoires pour contenir la clé d'utilisateur et la base de données de CSR :

```
[~/]$ mkdir -m 0755 \
```

```
~/examples/TestUser \
~/examples/TestUser/private \
~/examples/TestUser/certs
```

Copiez le fichier `openssl.cnf` modifié dans le répertoire de travail :

```
[~/examples]$ cp -v ~/examples/openssl.cnf ~/examples/TestUser/
`~/examples/openssl.cnf' -> `~/examples/TestUser/openssl.cnf'
```

Fourniture d'informations de certificat utilisateur x509

Les données peuvent être entrées manuellement lorsque vous y êtes invité ou fournies automatiquement via un fichier de configuration OpenSSL. Le fichier de configuration par défaut est suffisant.

Génération d'une CSR d'utilisateur et d'une nouvelle clé de serveur

Cette étape génère une nouvelle clé (`-newkey`) et génère une demande de certificat pour un utilisateur. Le certificat qui en résulte inclura le champ d'objet (`-subj`). Le champ d'objet peut être spécifié sur la ligne de commande OpenSSL comme un paramètre particulier, ou il peut être rempli à partir de différents champs dans le fichier `openssl.cnf`. (Pour plus d'informations, reportez-vous à la section « Méthodes de spécification du champ d'objet sur une CSR » (Méthodes de spécification du champ d'objet sur une CSR à la page 428)). `Le CSR est écrit dans le fichier spécifié par le paramètre - out`. Dans l'exemple de commande suivant, le champ d'objet est spécifié sous forme d'un paramètre unique, et la CSR est écrite dans `./temp-test-user.csr`.

```
[~/examples/TestUser]$ openssl req \
-subj "/O=Hewlett-Packard Company/OU=Employment Status - Employees/OU=VPN-WEB-H/CN=Jonathan Smith/emailAddress=jonathan.smith@hp.com" \
-config ./openssl.cnf \
-newkey rsa:2048 -sha256 \
-keyout ./private/test-user-private.key \
-nodes \
-out ./temp-test-user.csr
```

Affichez la CSR et vérifiez qu'elle correspond à ce que vous souhaitez signer. La commande suivante affiche la CSR :

```
[ ]$ openssl req -in ./temp-test-user.csr -text
```

Signature de la CSR d'utilisateur avec la clé level1CA

Pour signer et configurer un certificat utilisateur :

1. Signez la CSR d'utilisateur avec la clé `level1CA`, comme dans l'exemple suivant :

   ```
   [ ]$ cd ~/examples/level1CA/
   ```

2. Affichez la CSR et vérifiez qu'elle correspond à ce que vous souhaitez signer. La commande suivante affiche la CSR :

   ```
   [ level1CA]$ openssl req -in ../TestUser/temp-test-user.csr -text
   ```

3. Il est important de spécifier la manière dont le certificat utilisateur peut être utilisé. Effectuez cela à l'aide d'extensions x509. (Pour plus d'informations sur les extensions x509, consultez le site Web OpenSSL (http://www.openssl.org/docs/apps/x509v3_config.html#).) La différence entre un certificat de serveur et un certificat utilisateur est les autorisations que l'autorité de certification attribue au certificat. Par exemple, un certificat CA est généralement utilisé en tant que SSL serveur, alors qu'un certificat utilisateur doit être utilisé comme une connexion SSL de client et de carte à puce.

   Pour spécifier les extensions, modifiez la section `[ user_cert ]` du fichier `openssl.cnf`, comme illustré dans l'exemple suivant. Supprimez les commentaires des lignes `nsCertType` et `keyUsage` comme indiqué. Les lignes modifiées sont affichées en gras.

```
[ usr_cert ]

# These extensions are added when 'ca' signs a request.

# This goes against PKIX guidelines but some CAs do it and some
software

# requires this to avoid interpreting an end user certificate as a CA.

basicConstraints=critical, CA:FALSE

# Here are some examples of the usage of nsCertType. If it is omitted

# the certificate can be used for anything *except* object signing.

# This is OK for an SSL server.

# nsCertType = server

# For an object signing certificate this would be used.

# nsCertType = objsign

# For normal client use this is typical

nsCertType = client, email # Uncomment this line

# and for everything including object signing:

# nsCertType = client, email, objsign

# This is typical in keyUsage for a client certificate.

# Uncomment this line:

keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment

# If extendedKeyUsage is specified, it MUST include all three items

# to be used for Two-Factor authentication.

# Client Authentication (1.3.6.1.5.5.7.3.2)

# Code Signing (1.3.6.1.5.5.7.3.3)

# Smart Card Login (1.3.6.1.4.1.311.20.2.2)
```

```
#
extendedKeyUsage=clientAuth,codeSigning,1.3.6.1.4.1.311.20.2.2

# This will be displayed in Netscape's comment listbox.
nsComment = "OpenSSL Generated Certificate"

# PKIX recommendations harmless if included in all certificates.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

# This stuff is for subjectAltName and issuerAltname.
# Import the email address.
# subjectAltName=email:copy
# An alternative to produce certificates that aren't
# deprecated according to PKIX.
# subjectAltName=email:move

# Copy subject details
# issuerAltName=issuer:copy

# For testing purposes we will just use some well known CR
nsCaRevocationUrl = http://onsitecrl.verisign.com/
HewlettPackardCompanyITInfrastructure/LatestCRL.crl
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName
```

4. Signez la demande de certificat, comme dans l'exemple suivant :

```
[level1CA]$ openssl ca -config ./openssl.cnf -extensions usr_cert \-
policy policy_anything -in ../TestUser/temp-test-user.csr -cert \
certs/level1CA.pem -md sha256 -keyfile private/level1CA-private.key
```

5. Pour afficher les résultats, exécutez la commande suivante :

```
[ level1CA]$ openssl x509 -in newcerts/07.pem -noout -text
```

6. Pour activer l'utilisation de certificats dans des cartes à puce, le champ `keyUsage` doit inclure `sslAuth` et, s'il est présent, le champ `extendedKeyUsage` doit spécifier l'authentification des clients, la signature du code et la connexion de carte à puce. Pour plus d'informations, consultez la section « Résolution des problèmes d'authentification TFA et LDAP » (Résolution des problèmes d'authentification TFA et LDAP à la page 429).

7. Accordez le certificat public à l'utilisateur, à l'aide de la commande suivante :

```
[ TestUser]$ cp -v ~/examples/level1CA/newcerts/07.pem ~/examples/Test/User/certs/test-user.pem

`../level1CA/newcerts/06.pem' -> `certs/test-user.pem'
```

8. Combinez le certificat public et la clé privée en un fichier `.pem` PKCS #12 en créant un certificat PKCS #12 et en fournissant un mot de passe (PIN) pour le certificat. L'utilisateur est invité à entrer le mot de passe (PIN). Ce mot de passe protège la clé privée contenue dans le certificat PKCS #12.

```
[ ]$ cd ~/examples/TestUser

[ TestUser]$ openssl pkcs12 -export -in certs/test-user.pem -inkey \ private/test-user-private.key -out private/test-user-private.p12
```

Vérification de certificats

Pour vérifier les certificats, procédez comme suit.

1. Pour vérifier les certificats, utilisez les commandes indiquées dans l'exemple suivant :

```
[ examples]$ mkdir CA

[ examples]$ cp -v rootCA/certs/rootCA.crt CA/CA.pem

`rootCA/certs/rootCA.crt' -> `CA/CA.pem'

[ examples]$ cat level1CA/certs/level1CA.pem >> CA/CA.pem

[ examples]$ openssl verify -CAfile CA/CA.pem -verbose -purpose sslserver ./level1CA/certs/level1CA.pem

./level1CA/certs/level1CA.pem: OK
```

2. Vérifiez que le certificat utilisateur ne peut pas être utilisé pour des besoins de serveur SSL, comme cela est réalisé dans l'exemple suivant :

```
[examples]$ openssl verify -CAfile CA/CA.pem -verbose -purpose sslserver ./TestUser/certs/test-user.pem

./TestUser/certs/test-user.pem: /O=Hewlett-Packard Company/OU=Employment Status - Employees/OU=VPN-WEB-H/CN=Jonathan Smith/emailAddress=jonathan.smith@hp.com

error 26 at 0 depth lookup:unsupported certificate purpose

OK
```

Vérifiez que le certificat utilisateur peut être utilisé pour des besoins de client SSL :

```
[user1@user1-station examples]$ openssl verify -CAfile CA/CA.pem -verbose -purpose sslclient ./TestUser/certs/test-user.pem

./TestUser/certs/test-user.pem: OK
```

Stockage d'un certificat utilisateur sur une carte à puce ou un navigateur

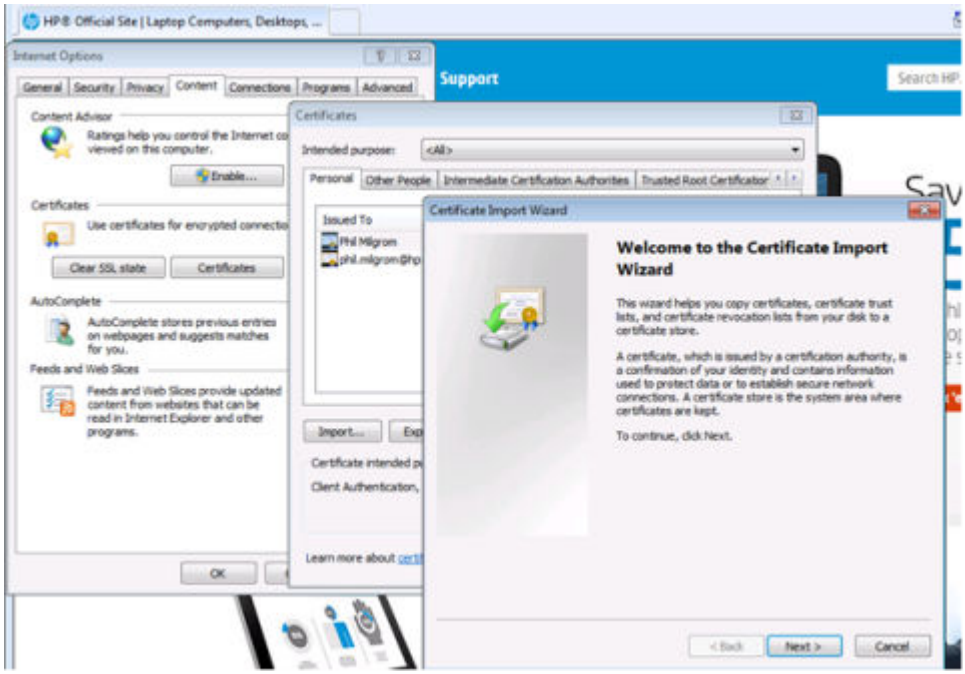
Cette section explique comment enregistrer un certificat utilisateur sur une carte à puce ou un navigateur. Les informations de navigateur dans cette section sont basées sur Microsoft Internet Explorer.

Microsoft Internet Explorer ne prend pas en charge les fichiers au format PEM. Créez un certificat `.p12` qui contient les clés privées et publiques, à l'aide d'une commande telle que la suivante :

```
[ TestUser]$ openssl pkcs12 -export -in certs/test-user.pem -inkey
private/test-user-private.key -out private/test-user-private.p12
```

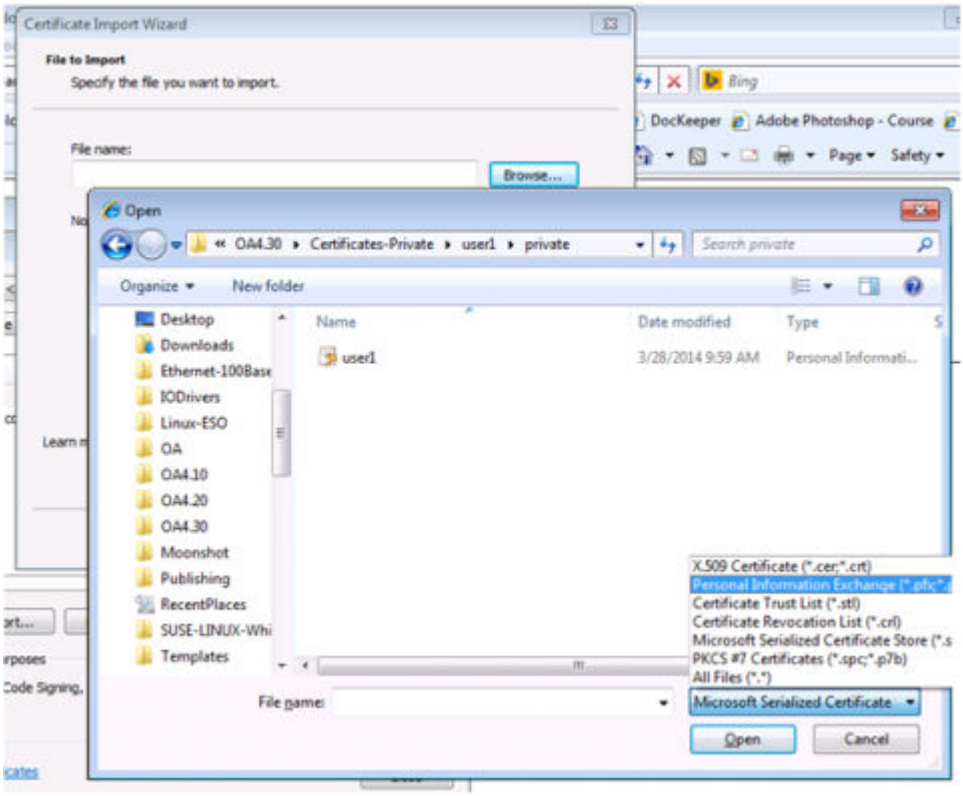
Pour installer le certificat `.p12` à l'aide d'Internet Explorer 8, procédez comme suit :

1. Accédez à l'Assistant d'importation de certificat de Internet Explorer Internet en cliquant sur **Outils>OptionsInternet>Contenu>Certificats** :



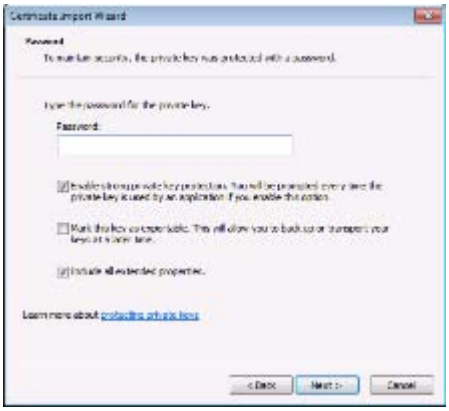
2. Cliquez sur **Next** (Suivant).
3. Cliquez sur **Browse** (Parcourir).
   a. Recherchez le répertoire qui contient le fichier de certificat `.p12`.

b. Modifiez le type de fichier en `Personal Information Exchange (.p12)`.



c. Sélectionnez le fichier de certificat `.p12` approprié.

4. Sélectionnez le fichier `.p12`, puis cliquez sur **Next** (Suivant).
5. Entrez le mot de passe spécifié lors de la création du fichier PKCS #12 (voir la section « Signature de la CSR d'utilisateur avec la clé level1CA » (Signature de la CSR d'utilisateur avec la clé level1CA à la page 413)), puis cliquez sur **Next** (Suivant). (Acceptez les valeurs de case à cocher par défaut.)



6. La fenêtre Certificate Store s'affiche. Cliquez sur **Next** (Suivant).
7. Pour terminer la procédure d'installation (importer) de l'Assistant, cliquez sur **Finish** (Terminer).

8. La fenêtre suivante indique qu'une application crée un élément protégé et que le niveau de sécurité est défini pour cet élément. Cliquez sur **OK**.
9. Lorsque l'Assistant indique que l'importation a réussi, cliquez sur **OK**.

Configuration du module Onboard Administrator pour l'authentification à deux facteurs avec comptes locaux

Cette section fournit un exemple illustrant la manière de configurer le module Onboard Administrator pour mettre en place l'authentification à deux facteurs.

Établissement d'un plan de récupération du module Onboard Administrator

HP recommande de mettre en place un plan de récupération avant la configuration du module Onboard Administrator pour l'authentification à deux facteurs de certificats. Si un problème quelconque se produit au cours de la configuration, la configuration du module Onboard Administrator peut être récupérée en accédant à l'unité de clé USB au travers du port série ou de l'écran Insight Display. Les deux méthodes exigent un accès physique au module Onboard Administrator.

REMARQUE : Si un PIN d'écran LCD a été configuré (et oublié) et que des comptes locaux ont été désactivés ou que la fonction TFA a été configurée de manière incorrecte, la seule manière d'effectuer une récupération est via un port série.

Les deux situations la plus courantes, dans lesquelles la récupération du module Onboard Administrator est nécessaire, sont lorsque LDAP a été configuré avec des comptes locaux désactivés ou lorsque l'authentification à deux facteurs a été configurée sans accès aux certificats (`keyUsage`).

Récupération via l'écran Insight Display et la clé USB

Pour récupérer le module Onboard Administratorvia une clé USB, créez un fichier de configuration sur la clé USB pour restaurer les paramètres nécessaires. Le fichier peut être configuré pour réinitialiser uniquement ce qui est requis pour rétablir l'accès ou pour restaurer complètement des paramètres usine :

- `GAIN_ACCESS.CFG` (réinitialiser uniquement ce qui est requis pour rétablir l'accès) :

  ```
  DISABLE TWOFACTOR

  DISABLE LDAP

  SET USER PASSWORD "Administrator" "My.Password123"
  ```

- `SET_FACTORY.CFG` (réinitialisation sur valeurs usine par défaut) :

  ```
  SET FACTORY
  ```

Pour récupérer une configuration :

1. Insérez la clé USB contenant le fichier de configuration dans le port USB du module Onboard Administrator.
2. À l'aide de l'écran Insight display, accédez au menu principal, sélectionnez **USB Key Menu**, puis cliquez sur **OK**.
3. Sélectionnez **Restore Configuration** (Restaurer la configuration), puis cliquez sur **OK**.
4. Sélectionnez le fichier de configuration répertorié, puis cliquez sur **OK**.
5. L'écran Confirm Details (Confirmer les détails) apparaît. Cliquez sur **OK**.

Récupération via la console série

Pour récupérer le module Onboard Administratorvia le port série, procédez comme suit :

1. Assurez-vous de disposer des logiciels et câbles appropriés pour vous connecter au port série du module Onboard Administrator. Le paramètre de connexion série par défaut est 9600, 8, N, 1. Pour plus d'informations, consultez la section « Récupération du mot de passe administrateur » (Récupération du mot de passe administrateur à la page 14).
2. Appuyez sur le bouton **Reset** et maintenez-le enfoncé pendant cinq secondes.
3. Sur la console série, lorsque vous êtes invité à choisir Flash Recovery (Récupération Flash) ou Reset Password (Réinitialiser mot de passe), appuyez sur la touche **L** (Lost Password - Mot de passe perdu).

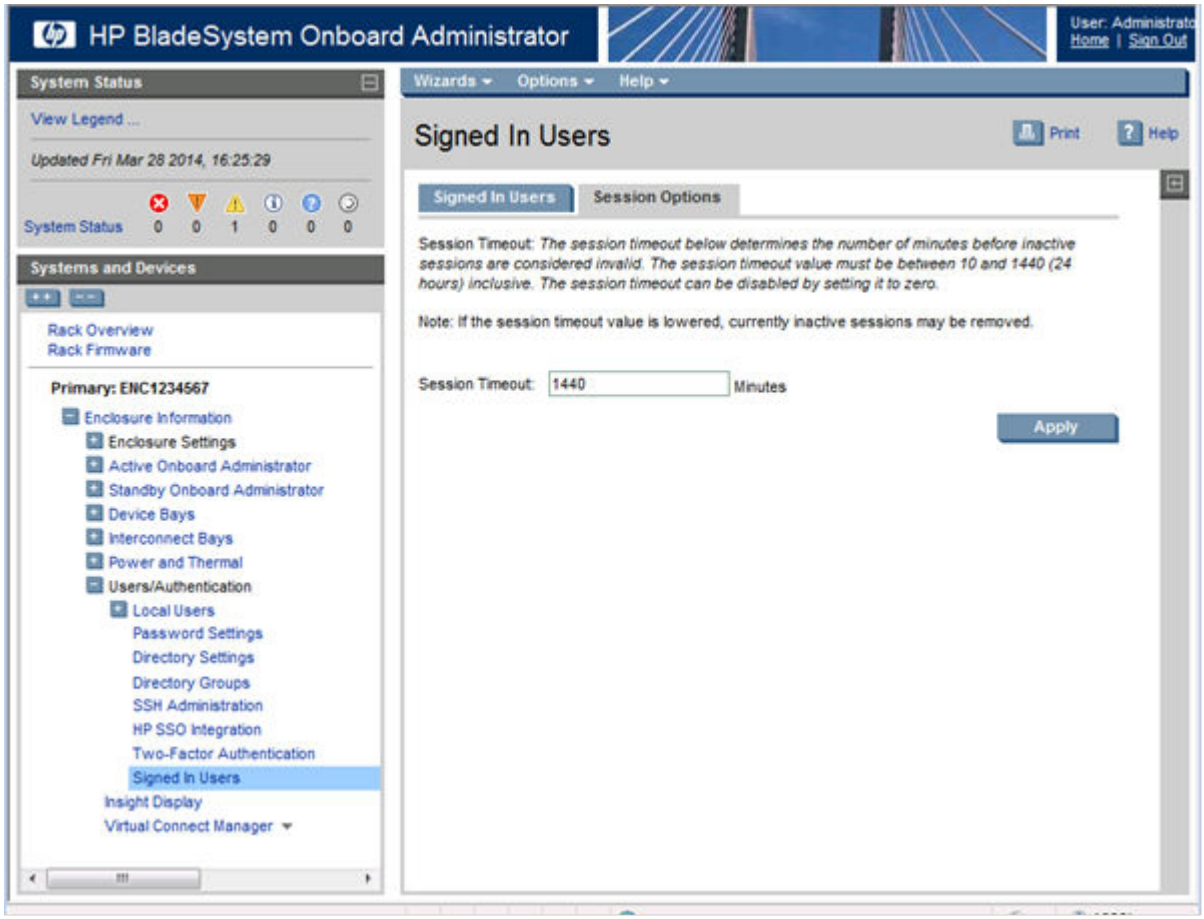
   La console affiche le mot de passe du compte administrateur intégré et les comptes locaux sont activés.

Configuration de l'expiration de la session Onboard Administrator

Par défaut, si une session d'utilisateur est inactive pour un jour (1440 minutes), un délai d'expiration se produit. Réduisez ce paramètre à une valeur qui convient à votre stratégie de sécurité. À des fins de test, vous pouvez définir la valeur de délai d'expiration à un minimum de 10 minutes. Pour modifier le paramètre de délai d'expiration, utilisez l'interface Onboard Administrator ou une commande CLI. Les valeurs de délai d'expiration valides sont 0 (ce qui désactive le délai d'expiration), ou un entier compris entre 10 et 1440.

Utilisation de l'interface utilisateur graphique

1. Accédez à l'écran **Signed in Users** (**Enclosure Information>Users/Authentication>Signed in Users**), puis sélectionnez l'onglet **Session Options**.



2. Modifiez le champ **Session Timeout** (Délai d'expiration de session).
3. Cliquez sur **Apply** (Appliquer).

Utilisation de l'interface CLI

Utilisez la commande suivante, où <*timeout-value*> correspond au nombre de minutes :

```
SET SESSION TIMEOUT<timeout-value>
```

Installation de la chaîne d'autorités de certification pour authentification à deux facteurs

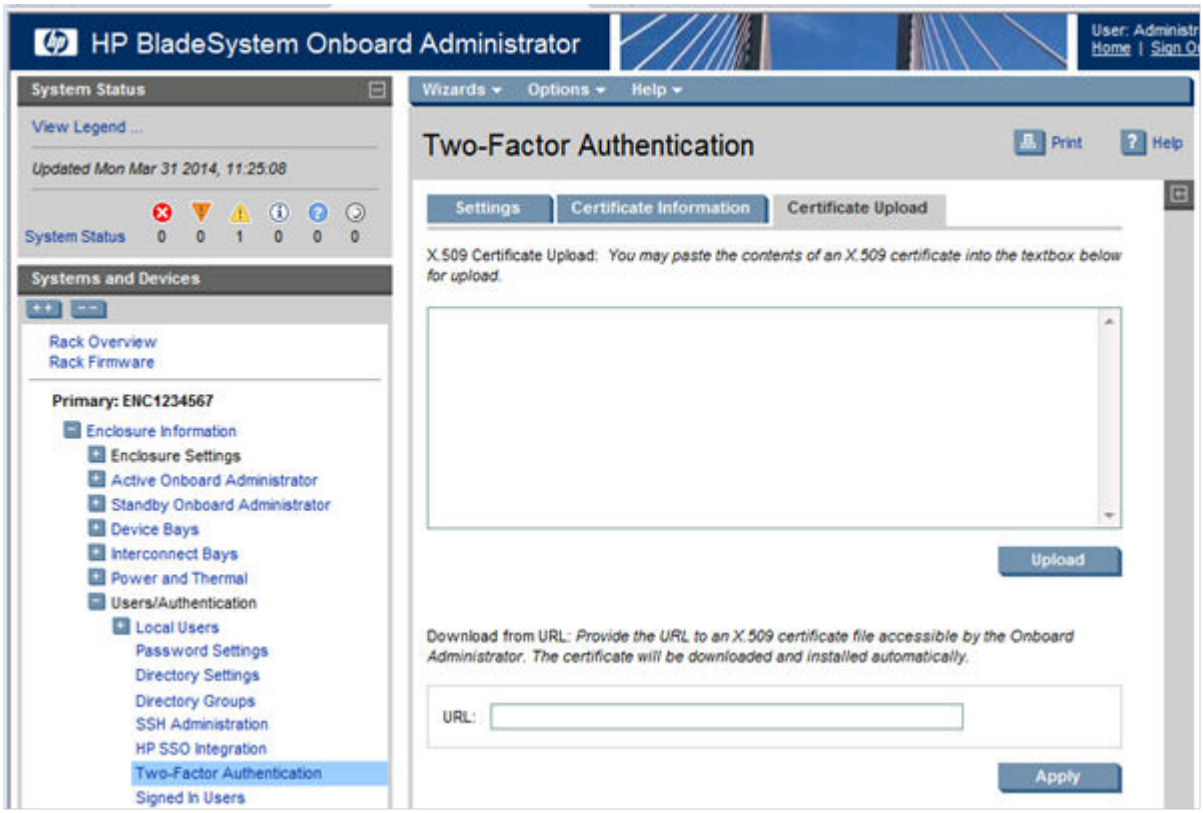
Une chaîne de certificats est constituée de tous les certificats nécessaires pour vérifier le certificat utilisateur. La chaîne de certificats commence par le certificat racine suivi de tous les certificats d'autorités intermédiaires. Chaque autorité de certification intermédiaire de la chaîne contient un certificat émis par l'autorité de certification qui est un niveau au-dessus de la hiérarchie de confiance. L'autorité de certification racine émet un certificat pour elle-même.

Cette section explique comment installer les autorités de certification pour l'authentification à deux facteurs.

REMARQUE : L'authentification à deux facteurs et le protocole LDAP ont des référentiels distincts pour les autorités de certification. Ne les confondez pas les uns avec les autres.

Pour installer des certificats d'autorité de certification pour l'authentification à deux facteurs, utilisez l'interface Onboard Administrator comme suit :

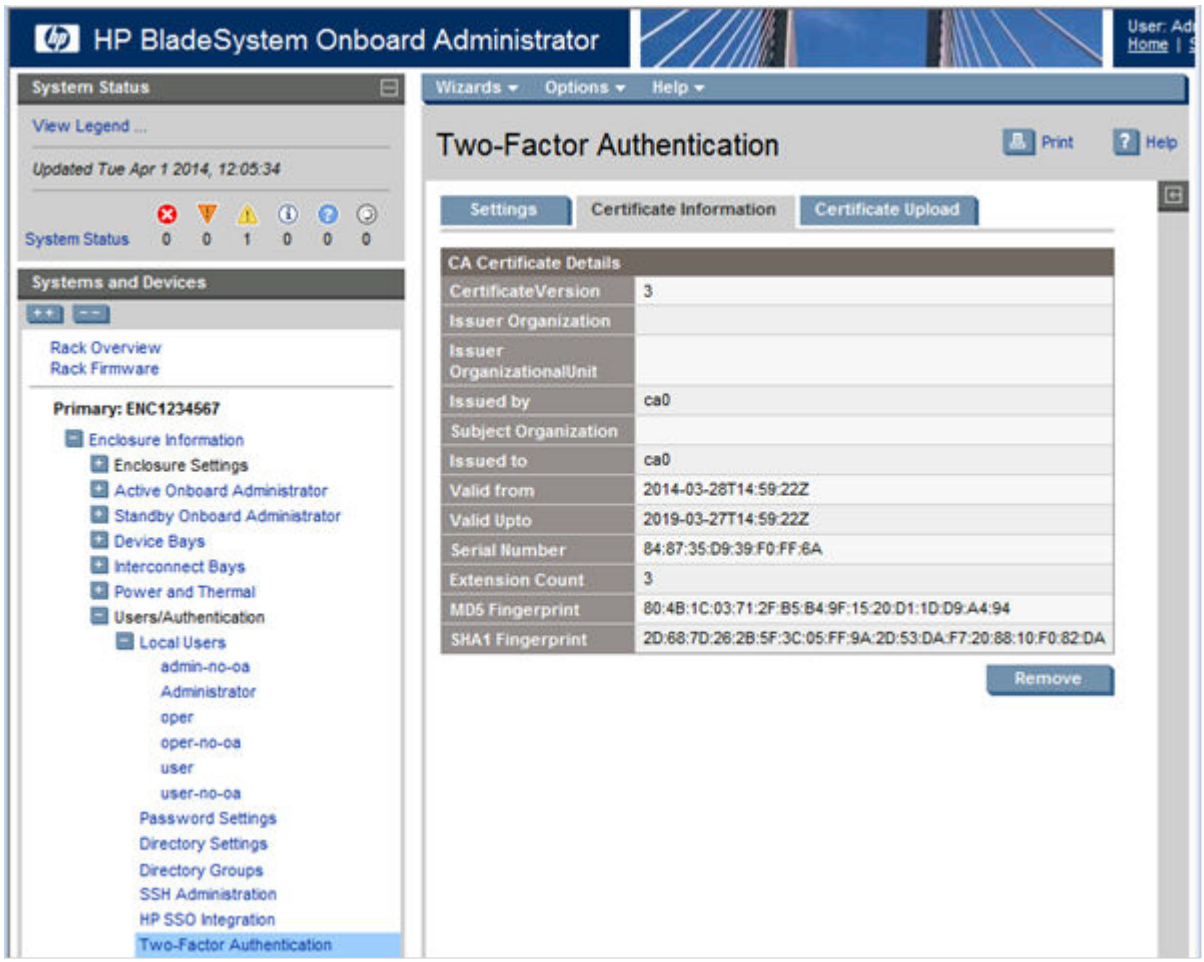
1. Accédez à l'écran de l'authentification à deux facteurs : **Enclosure Information>Users/ Authentication>Two-Factor Authentication**.
2. Cliquez sur l'onglet **Certificate Upload** (Téléchargement de certificat). L'écran **Certificate Upload** apparaît comme illustré dans l'exemple suivant.



3. Copiez et collez le certificat d'autorité de certification racine dans la zone de texte fournie par l'écran **Certificate Upload**. Le certificat comprend des délimiteurs de début et de fin, comme indiqué :

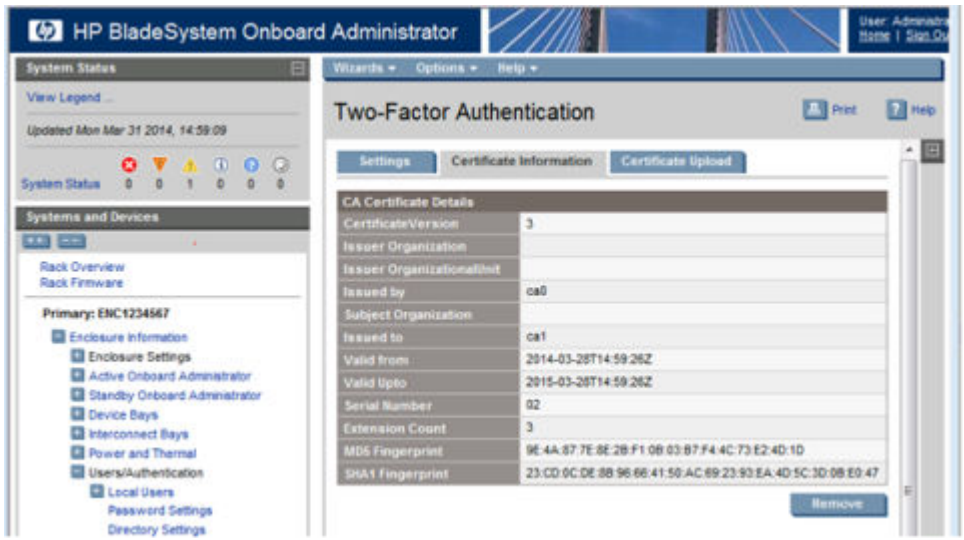
```
-----BEGIN CERTIFICATE-----

MIIDkTCCAnmgAwIBAgIJALg8cO2Ikvr8MA0GCSqGSIb3DQEBBQUAMDkxDDAKBgNV

BAMTA2NhMDEUMBIGCgmSJomT8ixkARkWBHRlc3QxEzARBgoJkiaJk/IsZAEZFgNj

.

.

.

Ob6IFCSUTKbCVT95cYTRHiSbgBYaqDXBJk3Lyjvtb7ZovmMT5dnU/w061wV5MEce

RZfXH3U=

-----END CERTIFICATE-----
```

4. Cliquez sur **Upload** (Charger). Une fois le certificat chargé avec succès, l'onglet **Certificate Information** s'affiche, comme dans l'exemple suivant.



5. Ajoutez une autorité de certification intermédiaire ou de fin dans la chaîne :
   a. Revenez à l'onglet **Certificate Upload**.
   b. Copiez et collez le certificat d'autorité de certification suivant dans la zone de texte fournie.

c. Cliquez sur **Upload** (Charger). Une fois le certificat chargé avec succès, l'onglet **Certificate Information** s'affiche, comme dans l'exemple suivant (dans cet exemple, le certificat CA1 a été émis par l'autorité de certification racine CA0).



d. Pour installer des autorités supplémentaires, répétez les étapes a à c pour chaque certificat intermédiaire.

Commandes CLI pour administration de certificats

Utilisez les commandes CLI suivantes pour ajouter, télécharger, afficher et supprimer des certificats. Pour plus d'informations, consultez le *Manuel de l'utilisateur de l'interface de ligne de commande HP BladeSystem Onboard Administrator*.

- `ADD CA CERTIFICATE`
- `DOWNLOAD CA CERTIFICATE`
- `SHOW CA CERTIFICATE`
- `REMOVE CA CERTIFICATE`

Configuration du proxy HTTP

Le module Onboard Administrator peut nécessiter un serveur proxy pour accéder à des adresses telles que celles nécessaire pour vérifier un certificat ou pour obtenir une liste CRL. (Une liste CRL est une base de données de certificats qui ont été révoqués avant leur arrivée à expiration.) Pour ce faire, configurez le serveur de proxy HTTP sur le module Onboard Administrator à l'aide de la commande suivante :

`SET URB PROXY URL { <URL> }`

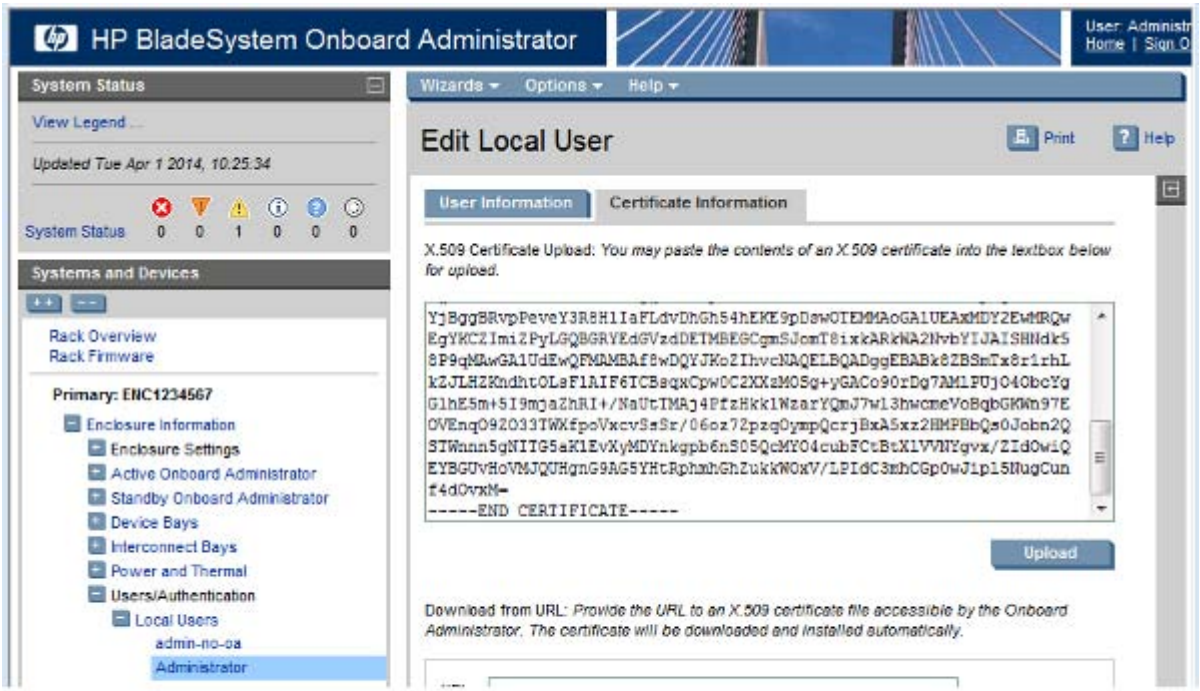
L'URL spécifiée peut comporter jusqu'à 128 caractères.

L'interface Onboard Administrator n'inclut pas la possibilité de définir une URL de proxy.

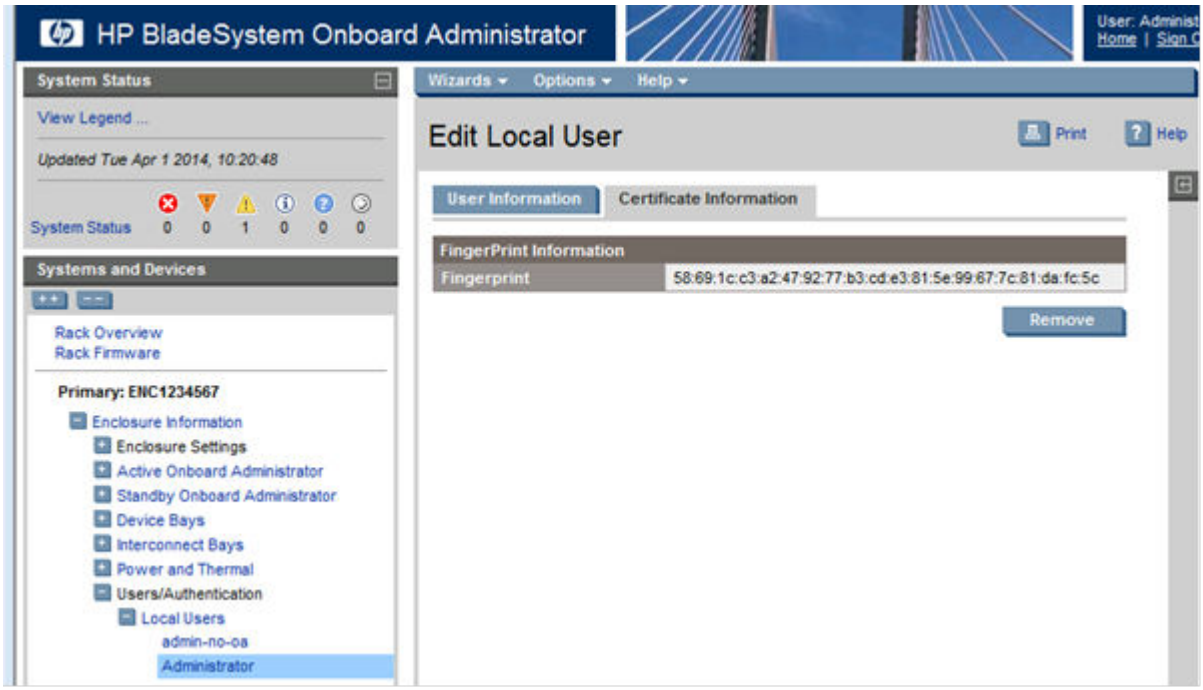
Installation de certificats utilisateur sur le compte administrateur local

Installez un certificat utilisateur sur le compte administrateur du module Onboard Administrator Administrator, en procédant comme suit :

1. Accédez à l'écran Local Users Administrator (Edit Local User) : **Enclosure Information>Users/Authentication>Local Users>Administrator**.
2. Cliquez sur l'onglet **Certificate Information**. Si aucun certificat d'administrateur n'a encore été installé, l'écran **Certificate Information** s'affiche avec une zone de texte vide. Copiez et collez le certificat utilisateur approprié dans la zone de texte, comme indiqué.



3. Cliquez sur **Upload** (Charger). Une fois le certificat chargé avec succès, l'onglet **Certificate Information** s'affiche, comme dans l'exemple suivant :



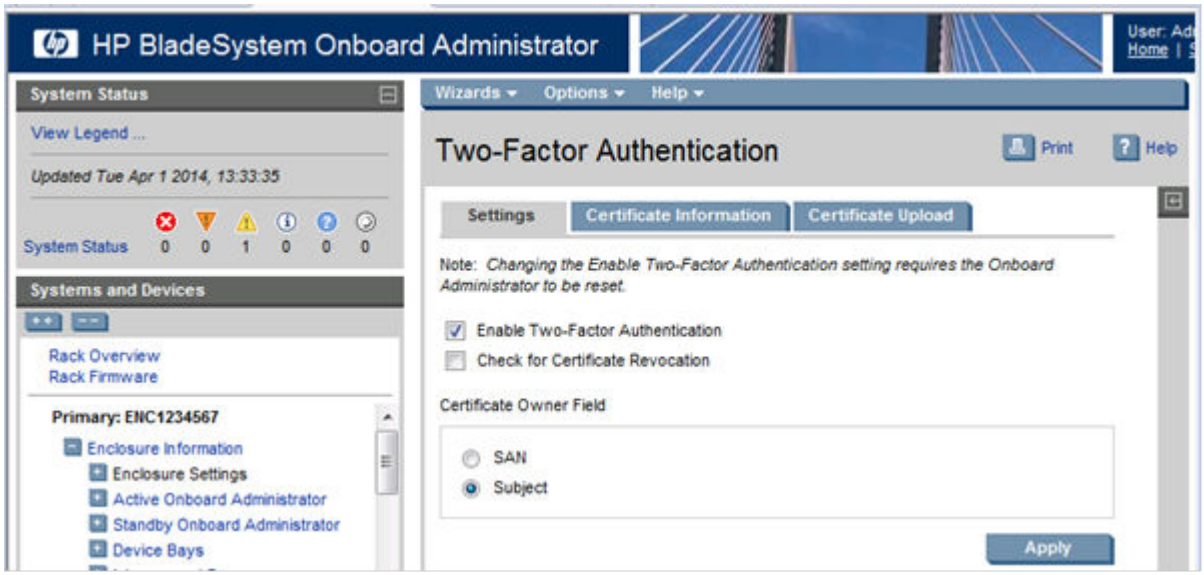
Si le certificat utilisateur chargé ne peut pas être vérifié, consultez la section « Divers problèmes connus » (Problèmes connus divers à la page 393).

Activation de l'authentification à deux facteurs

Après le succès du chargement de certificats d'autorité de certification pour l'authentification à deux facteurs et le chargement d'au moins un compte administrateur du module Onboard Administrator, vous pouvez activer l'authentification à deux facteurs :

1. Accédez à l'onglet **Two-Factor Authentication Settings** (cliquez sur **Enclosure Information>Users/Authentication>Local Users>Two-Factor Authentication**).

   Cochez la case **Enable Two-Factor Authentication**, comme indiqué dans l'exemple suivant. Si vous utilisez l'authentification à deux facteurs en combinaison avec LDAP, spécifiez dans la zone **Certificate Owner Field** si le module Onboard Administrator doit utiliser le champ de nom alternatif d'objet (**SAN**) ou le champ d'objet de certificat (**Subject**). Pour plus d'informations sur l'utilisation de l'authentification à deux facteurs avec LDAP, reportez-vous à la section « Authentification TFA+LDAP » (Authentification TFA+LDAP à la page 427).



2. Cliquez sur **Apply** (Appliquer).

Connexion à l'interface Web Onboard Administrator à l'aide de l'authentification à deux facteurs

Accédez à l'interface utilisateur Web du module Onboard Administrator et cliquez sur le certificat utilisateur approprié (s'il y a plusieurs serveurs). Le navigateur doit vous inviter à confirmer le certificat.

Le certificat est nécessaire pour établir une session SSL/TLS avec le module Onboard Administrator. Si la connexion est établie avec succès, vous êtes connecté au module Onboard Administrator sous le compte d'utilisateur local associé au certificat utilisateur.

En cas de problème, consultez la section « Résolution des problèmes d'authentification TFA et LDAP » (Résolution des problèmes d'authentification TFA et LDAP à la page 429).

Authentification TFA+LDAP

En plus de l'Authentification à deux facteurs normale, le module Onboard Administrator prend également en charge l'authentification TFA+LDAP. Dans ce mode, l'utilisateur doit :

- Disposer d'un certificat utilisateur installé sur le module Onboard Administrator
- Connaître le code PIN d'accès au certificat
- Connaître le mot de passe de l'utilisateur LDAP associé

Les avantages de l'authentification TFA+LDAP sont :

- Une plus grande sécurité est obtenue dans la mesure où trois éléments doivent être authentifiés au lieu de deux.
- L'autorisation (autorisation d'accès) est gérée à l'aide de groupes LDAP au lieu d'un mappage de certificats utilisateur sur des comptes utilisateurs Onboard Administrator locaux individuels.

Fonctionnement de l'authentification TFA+LDAP

Si LDAP est configuré et que le certificat utilisateur de l'authentification à deux facteurs n'est pas mappé sur un compte utilisateur local du module Onboard Administrator, lorsqu'un utilisateur essaie de se connecter à la page de connexion d'interface du module Onboard Administrator, ce dernier extrait un ID utilisateur à partir du certificat utilisateur et invite l'utilisateur à fournir le mot de passe LDAP.

Le nom d'utilisateur LDAP est extrait à partir de l'objet ou champ de nom alternatif d'objet du certificat et est visible dans la page de connexion du module Onboard Administrator, en fonction de votre sélection effectuée sur l'onglet Two-Factor Authentication Settings. Pour plus d'informations, consultez la section « Activation de l'authentification à deux facteurs » (Activation de l'authentification à deux facteurs à la page 426). Si l'objet est sélectionné, le nom d'utilisateur est formaté selon la norme RFC 2253 pour créer un nom de domaine complet (FQDN). Si **SAN** (nom d'objet alternatif) est sélectionné, le module Onboard Administrator utilise le premier champ SAN dans le certificat qui est de type EMAIL, OTHERNAME, DNS ou URI. L'autorité de certification contrôle l'ordre et le contenu des champs de nom alternatif d'objet pendant le processus de signature. Vous ne pouvez pas modifier le nom utilisé dans l'interface utilisateur.

Une fois que vous spécifiez le mot de passe LDAP, les contrôles suivants se produisent :

- Le certificat utilisateur est comparé aux certificats d'autorité de certification installés sur le module Onboard Administrator.
- Les informations d'identification LDAP sont authentifiées sur le serveur LDAP configuré.
- L'utilisateur LDAP est vérifié en tant que membre d'un groupe autorisé sur le module Onboard Administrator.

Si les trois conditions sont remplies, une session sur le module Onboard Administrator est établie et l'utilisateur est connecté au module Onboard Administrator.

Activation de l'authentification TFA+LDAP

Pour utiliser l'authentification TFA+LDAP, procédez comme suit :

1. Configurez le module Onboard Administrator pour l'authentification à deux facteurs, en suivant les instructions indiquées dans la section « Configuration du module Onboard Administrator pour l'authentification à deux facteurs avec comptes locaux » (Configuration du module Onboard Administrator pour l'authentification à deux facteurs avec comptes locaux à la page 419).
2. Configurez le module Onboard Administrator pour utiliser l'authentification LDAP, tel que décrit dans la section « Écran Directory Settings » (Écran Directory Settings à la page 334).
3. Connectez-vous au module Onboard Administrator à l'aide uniquement de l'authentification à deux facteurs, puis réactivez LDAP (requis car l'activation de l'authentification à deux facteurs désactive automatiquement LDAP). Pour plus d'informations sur l'activation de LDAP, consultez les sections « Écran Directory Settings » (Écran Directory Settings à la page 334) et « Préparation de l'annuaire » (Préparation de l'annuaire à la page 396).
4. Après avoir vérifié que tout fonctionne comme prévu, vous pouvez désactiver l'accès des comptes locaux en désactivant la case à cocher **Enable Local Users** sur l'écran Directory Settings.

Méthodes de spécification du champ d'objet sur une CSR

Utilisez une de différentes méthodes pour contrôler le contenu du champ d'**objet** sur une CSR :

- Mode interactif sur la ligne de commande OpenSSL
- Manuellement sur la ligne de commande OpenSSL (pour un exemple, voir la section « Génération d'une CSR d'utilisateur et d'une nouvelle clé de serveur » (Génération d'une CSR d'utilisateur et d'une nouvelle clé de serveur à la page 413))
- Dans le fichier de configuration OpenSSL (`.cnf`)
- Au travers d'un fichier de réponse OpenSSL abrégé (le fichier de réponse est généré par l'autorité de certification et contient votre clé publique et est signé numériquement par l'autorité de certification ; vous devez installer le fichier de réponse sur le serveur Web)

Utilisez la méthode la mieux adaptée à vos besoins.

Résolution des problèmes d'authentification TFA et LDAP

Cette section décrit des solutions aux problèmes qui peuvent s'afficher lorsque vous tentez une authentification à l'aide de certificats TFA et LDAP.

Problème : Le navigateur indique un message `cannot display webpage` (impossible d'afficher page Web) ou `authentication attempt failed` (échec de tentative d'authentification).

Solution : Pour le problème `cannot display webpage` :

1. Vérifiez que le certificat a une utilisation approuvée pour le client SSL. Par exemple, émettez la commande suivante :

   ```
   [ examples]$ openssl verify -CAfile CA/CA.pem -verbose  \ -purpose sslclient ./TestUser/
   certs/test-user.pem

   ./TestUser/certs/test-user.pem: OK
   ```

2. Vérifiez que ce certificat est disponible pour le navigateur. (Dans Internet Explorer, reportez-vous à **Outils > Options Internet > Contenu > Certificats**.)
3. Si le certificat est stocké sur une clé ou un jeton, assurez-vous qu'il a été correctement installé sur la clé ou le jeton.

Si vous voyez le message `authentication attempt failed` à partir du navigateur, un certificat avec utilisation du client SSL était disponible pour établir la session SSL/TLS, mais d'autres problèmes existent. Essayez les étapes suivantes :

1. Assurez-vous que le certificat est valide, à l'aide d'une commande telle que la suivante :

   ```
   [level1CA]$ openssl verify -CAfile CA/CA.pem -verbose -purpose sslclient ~/
   examples/level1CA/newcerts/0A.pem

   ..

   .

   error 9 at 0 depth lookup:certificate is not yet valid
   ```

2. Si le certificat n'est pas valide, suivez les instructions fournies par le message d'erreur OpenSSL. Si le certificat n'est pas valide, l'horloge système peut être défectueuse. Si le certificat ne peut pas être vérifié, le certificat d'autorité de certification correspondant peut ne pas être disponible. Pour cela, essayez ces étapes :

   a. Assurez-vous que les dates associées au certificat n'ont pas expiré.

   b. Examinez les champs `keyUsage` et `extendedKeyUsage` du fichier de configuration OpenSSL de la CSR. Le champ `keyUsage` spécifie les restrictions d'utilisation. S'il est

présent, le champ `extendedKeyUsage` place des restrictions supplémentaires sur l'utilisation.

Si le champ `extendedKeyUsage` est présent et spécifie `clientAuth` uniquement, le navigateur (Internet Explorer) ne passe pas le certificat au module Onboard Administrator. Cela entraîne le message `cannot display web page`.

Si le champ `extendedKeyUsage` n'est pas présent, le certificat peut être utilisé pour la connexion de carte à puce. Pour activer l'utilisation de certificats dans des cartes à puce, le champ `keyUsage` doit inclure `sslAuth` et, s'il est présent, le champ `extendedKeyUsage` doit spécifier l'authentification des clients, la signature du code et la connexion de carte à puce.

Exemples :

Le certificat suivant ne fonctionne pas car l'utilisation sslClient est manquante :

```
X509v3 Key Usage: critical

 Digital Signature, Non Repudiation
```

Le certificat suivant fonctionnera car il contient tous les éléments nécessaires :

```
X509v3 Extended Key Usage:

 TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin

 X509v3 Key Usage: critical

 Digital Signature, Non Repudiation, Key Encipherment
```

Problème : Problèmes de tentatives de basculement entre plusieurs utilisateurs client sur le même système.

Solution : Il arrive parfois que des navigateurs mettent en cache des informations d'identification selon une mesure plus étendue que nécessaire. Essayez d'effacer le cache du navigateur, en supprimant tous les fichiers temporaires, puis en fermant toutes les fenêtres du navigateur. Sinon, le problème peut être résolu simplement en attendant pendant un jour que les sessions expirent.

Pour tester plusieurs certificats de client à partir du même système client, différentes connexions peuvent s'avérer nécessaires. Sinon, le navigateur peut sélectionner le dernier certificat valide connu.

Exemples de l'interface CLI pour configuration d'un compte utilisateur et de certificats

L'exemple suivant montre des commandes de l'interface CLI Onboard Administrator utilisées pour la configuration d'un compte d'utilisateur local et de certificats. Des commentaires suivent l'exemple.

```
=====================================

== Add user, CA certs, and user cert

=====================================

set script mode on

add user "marc" "password"

set user contact "marc" "800-555-1212"
```

```
set user fullname "marc" "Marc Last-name"

set user access "marc" ADMINISTRATOR

enable user "marc"

assign server all "marc"

assign interconnect all "marc"

assign oa "marc"

show user "marc"

download ca certificate http://dev-srvr/certs/Common-Policy.cer

download ca certificate http://dev-srvr/certs/SHA-1-Federal-Root-CA.cer

download ca certificate http://dev-srvr/certs/DoD-Interoperability-Root-
CA-1.cer

download ca certificate http://dev-srvr/certs/DoD-Root-CA-2.cer

download ca certificate http://dev-srvr/certs/DOD-EMAIL-CA-19.cer

download user certificate "marc" http://dev-srvr/certs/Marc-Lastname.cer

show user "marc"

set script mode off

================================================

== Go to the GUI, enable TFA, then

== log in via the Web browser using the TFA token.

================================================

=======================================

== Remove Fed certificates and user

=======================================

set script mode on

remove ca certificate "CD:78:54:4C:CA:C6:EA:15:72:81:86:EB:
86:59:F6:E6:C0:FA:A7:41"

remove ca certificate "B1:10:5C:D1:0F:C3:70:F5:6B:89:DD:1D:49:F6:D8:30:DF:
35:F2:DE"

remove ca certificate "FD:F3:F4:F8:C7:3B:5A:
63:20:62:08:88:29:00:D1:92:B1:75:BA:E8"

remove ca certificate "30:BE:4D:
40:F6:10:E5:65:B3:53:F3:44:C7:27:64:1E:EE:E7:86:D2"

remove ca certificate "CB:44:A0:97:85:7C:45:FA:18:7E:D9:52:08:6C:B9:84:1F:
2D:51:B5"

remove user certificate "Marc"

remove user "marc"
```

```
set script mode off
```

Les commandes dans la première section de l'exemple ajoutent un utilisateur avec des privilèges d'administrateur et installent des certificats :

- Ajoute un compte utilisateur (`ADD USER`)
- Définit des propriétés d'utilisateur (`SET USER`)
- Active un compte utilisateur (`ENABLE USER`)
- Affecte toutes les baies de serveur et d'interconnexion au contrôle de l'utilisateur (`ASSIGN SERVER ALL, ASSIGN INTERCONNECT ALL`)
- Accorde le privilège d'accès de l'utilisateur spécifié à des baies du module Onboard Administrator (`ASSIGN OA`)
- Affiche des informations utilisateur, un niveau d'accès utilisateur et des baies affectées à l'utilisateur (`SHOW USER`)
- Installe des certificats d'autorité de certification à partir des emplacements spécifiés (`DOWNLOAD CA CERTIFICATE`)
- Installe un certificat utilisateur à partir de l'emplacement spécifié (`DOWNLOAD USER CERTIFICATE`)

Les commentaires de script sont un rappel pour utiliser l'interface Onboard Administrator pour activer l'authentification à deux facteurs, puis se connecter via le navigateur Web, à l'aide de la touche TFA appropriée.

La deuxième section de l'exemple :

- Retire les certificats d'autorité de certification (`REMOVE CA CERTIFICATE`)
- Retire un certificat utilisateur (`REMOVE USER CERTIFICATE`)
- Retire un utilisateur (`REMOVE USER`)

Informations sur les autorités de certification et les certificats disponibles à partir du Web

Pour plus d'informations sur la gestion d'autorités de certification et de certificats, consultez les sites Web suivants :

- Site Web de documentation OpenSSL (http://www.openssl.org/docs)
- Site Web du Projet de documentation Linux (http://www.tldp.org/HOWTO/SSL-Certificates-HOWTO) (Comment gérer des autorités de certification et émettre ou signer des certificats SSL)
- Site Web G-Loaded Journal (http://www.g-loaded.eu/2005/11/10/be-your-own-ca/) (Comment devenir une autorité de certification et émettre des certificats de serveur)
- Site Web Debian Administration (http://www.debian-administration.org/articles/284) (Création et utilisation de certificats auto-signés)

14 Paramètres des fuseaux horaires

Paramètres de fuseaux horaires universels

REMARQUE : Les fuseaux horaires doivent être saisis exactement tels qu'ils s'affichent.

Le tableau suivant fournit les paramètres des fuseaux horaires universels pris en charge par le module Onboard Administrator.

CET	Etc/GMT+2	Etc/GMT+8	Etc/UCT	MST
CST6CDT	Etc/GMT-3	Etc/GMT-9	Etc/Universal	MST7MDT
EET	Etc/GMT+3	Etc/GMT+9	Etc/UTC	Navajo
EST	Etc/GMT-4	Etc/GMT-10	Etc/Zulu	PST8PDT
EST5EDT	Etc/GMT+4	Etc/GMT+10	Usine	UCT
Etc/GMT	Etc/GMT-5	Etc/GMT-11	GMT	Universal
Etc/GMT0	Etc/GMT+5	Etc/GMT+11	GMT+0	UTC
Etc/GMT-0	Etc/GMT-6	Etc/GMT-12	GMT0	WET
Etc/GMT+0	Etc/GMT+6	Etc/GMT+12	GMT-0	W-SU
Etc/GMT-1	Etc/GMT-7	Etc/GMT-13	Greenwich	Zulu
Etc/GMT+1	Etc/GMT+7	Etc/GMT-14	HST	—
Etc/GMT-2	Etc/GMT-8	Etc/Greenwich	MET	—

Paramètres de fuseaux horaires de la zone Afrique

REMARQUE : Les fuseaux horaires doivent être saisis exactement tels qu'ils s'affichent.

Le tableau suivant fournit les paramètres des fuseaux horaires africains pris en charge par le module Onboard Administrator.

Africa/Abidjan	Africa/Ceuta	Africa/Kinshasa	Africa/Niamey
Africa/Accra	Africa/Conakry	Africa/Lagos	Africa/Nouakchott
Africa/Addis_Ababa	Africa/Dakar	Africa/Libreville	Africa/Ouagadougou
Africa/Algiers	Africa/Dar_es_Salaam	Africa/Lome	Africa/Porto-Novo
Africa/Asmara	Africa/Djibouti	Africa/Luanda	Africa/Sao_Tome
Africa/Asmera	Africa/Douala	Africa/Lubumbashi	Africa/Timbuktu
Africa/Bamako	Africa/El_Aaiun	Africa/Lusaka	Africa/Tripoli
Africa/Bangui	Africa/Freetown	Africa/Malabo	Africa/Tunis
Africa/Banjul	Africa/Gaborone	Africa/Maputo	Africa/Wjndhoek

Africa/Bissau	Africa/Harare	Africa/Maseru	Egypt
Africa/Blantyre	Africa/Johannesburg	Africa/Mbabane	Libya
AfricaBrazzaville	Africa/Juba	Africa/Mogadishu	—
Africa/Bujumbura	Africa/Kampala	Africa/Monrovia	—
Africa/Cairo	Africa/Khartoum	Africa/Nairobi	—
Africa/Casablanca	Africa/Kigali	Africa/Ndjamena	—

Paramètres de fuseaux horaires de la zone Amérique

REMARQUE : Les fuseaux horaires doivent être saisis exactement tels qu'ils s'affichent.

Le tableau suivant fournit les paramètres des fuseaux horaires de la zone Amérique pris en charge par le module Onboard Administrator.

America/Adak	America/Guatemala	America/Rainy_River
America/Anchorage	America/Guayaquil	America/Rankin_Inlet
America/Anguilla	America/Guyana	America/Recife
America/Antigua	America/Halifax	America/Regina
America/Araguaina	America/Havana	America/Resolute
America/Argentina/Buenos_Aires	America/Hermosillo	America/Rio_Branco
America/Argentina/Catamarca	America/Indiana/Indianapolis	America/Rosario
America/Argentina/ComodRivadavia	America/Indiana/Knox	America/Santa_Isabel
America/Argentina/Cordoba	America/Indiana/Marengo	America/Santarem
America/Argentina/Jujuy	America/Indiana/Petersburg	America/Santiago
America/Argentina/La_Rioja	America/Indiana/Tell_City	America/Santo_Domingo
America/Argentina/Mendoza	America/Indiana/Vevay	America/Sao_Paulo
America/Argentina/Rio_Gallegos	America/Indiana/Vincennes	America/Scoresbysund
America/Argentina/Salta	America/Indiana/Winamac	America/Shiprock
America/Argentina/San_Juan	America/Indianapolis	America/Sitka
America/Argentina/San_Luis	America/Inuvik	America/St_Barthelemy
America/Argentina/Tucuman	America/Iqaluit	America/St_Johns
America/Argentina/Ushuaia	America/Jamaica	America/St_Kitts
America/Aruba	America/Jujuy	America/St_Lucia
America/Asuncion	America/Juneau	America/St_Thomas
America/Atikokan	America/Kentucky/Louisville	America/St_Vincent
America/Atka	America/Kentucky/Monticello	America/Swift_Current
America/Bahia	America/Knox_IN	America/Tegucigalpa

America/Bahia_Banderas	America/Kralendijk	America/Thule
America/Barbados	America/La_Paz	America/Thunder_Bay
America/Belem	America/Lima	America/Tijuana
America/Belize	America/Los_Angeles	America/Toronto
America/Blanc-Sablon	America/Louisville	America/Tortola
America/Boa_Vista	America/Lower_Princes	America/Vancouver
America/Bogota	America/Maceio	America/Virgin
America/Boise	America/Managua	America/Whitehorse
America/Buenos_Aires	America/Manaus	America/Winnipeg
America/Cambridge_Bay	America/Marigot	America/Yakutat
America/Campo_Grande	America/Martinique	America/Yellowknife
America/Cancun	America/Matamoros	Brazil/Acre
America/Caracas	America/Mazatlan	Brazil/DeNoronha
America/Catamarca	America/Mendoza	Brazil/East
America/Cayenne	America/Menominee	Brazil/West
America/Cayman	America/Merida	Canada/Atlantic
America/Chicago	America/Metlakatla	Canada/Central
America/Chihuahua	America/Mexico_City	Canada/Eastern
America/Coral_Harbour	America/Miquelon	Canada/East-Saskatchewan
America/Cordoba	America/Moncton	Canada/Mountain
America/Costa_Rica	America/Monterrey	Canada/Newfoundland
America/Creston	America/Montevideo	Canada/Pacific
America/Cuiaba	America/Montreal	Canada/Saskatchewan
America/Curacao	America/Montserrat	Canada/Yukon
America/Danmarkshavn	America/Nassau	Chile/Continental
America/Dawson	America/New_York	Chile/EasterIsland
America/Dawson_Creek	America/Nipigon	Cuba
America/Denver	America/Nome	Jamaica
America/Detroit	America/Noronha	Mexico/BajaNorte
America/Dominica	America/North_Dakota/Beulah	Mexico/BajaSur
America/Edmonton	America/North_Dakota/Center	Mexico/General
America/Eirunepe	America/North_Dakota/New_Salem	US/Alaska
America/El_Salvador	America/Ojinaga	US/Aleutian
America/Ensenada	America/Panama	US/Arizona
America/Fort_Wayne	America/Pangnirtung	US/Central

America/Fortaleza	America/Paramaribo	US/Eastern
America/Glace_Bay	America/Phoenix	US/East-Indiana
America/Godthab	America/Port_of_Spain	US/Indiana-Starke
America/Goose_Bay	America/Port-au-Prince	US/Michigan
America/Grand_Turk	America/Porto_Acre	US/Mountain
America/Grenada	America/Porto_Velho	US/Pacific
America/Guadeloupe	America/Puerto_Rico	US/Pacific-New

Paramètres de fuseaux horaires de la zone Asie

REMARQUE : Les fuseaux horaires doivent être saisis exactement tels qu'ils s'affichent.

Le tableau suivant fournit les paramètres des fuseaux horaires de la zone Asie pris en charge par le module Onboard Administrator.

Asia/Aden	Asia/Dhaka	Asia/Khandyga	Asia/Qyzylorda	Asia/Ulaanbaatar
Asia/Almaty	Asia/Dili	Asia/Kolkata	Asia/Rangoon	Asia/Ulan_Bator
Asia/Amman	Asia/Dubai	Asia/Krasnoyarsk	Asia/Riyadh	Asia/Urumqi
Asia/Anadyr	Asia/Dushanbe	Asia/Kuala_Lumpur	Asia/Riyadh87	Asia/Ust-Nera
Asia/Aqtau	Asia/Gaza	Asia/Kuching	Asia/Riyadh88	Asia/Vientiane
Asia/Aqtobe	Asia/Harbin	Asia/Kuwait	Asia/Riyadh89	Asia/Vladivostok
Asia/Ashgabat	Asia/Hebron	Asia/Macao	Asia/Saigon	Asia/Yakutsk
Asia/Ashkhabad	Asia/Ho_Chi_Minh	Asia/Macau	Asia/Sakhalin	Asia/Yekaterinburg
Asia/Baghdad	Asia/Hong_Kong	Asia/Magadan	Asia/Samarkand	Asia/Yerevan
Asia/Bahrain	Asia/Hovd	Asia/Makassar	Asia/Seoul	Hongkong
Asia/Baku	Asia/Irkutsk	Asia/Manila	Asia/Shanghai	Iran
Asia/Bangkok	Asia/Istanbul	Asia/Muscat	Asia/Singapore	Israel
Asia/Beirut	Asia/Jakarta	Asia/Nicosia	Asia/Taipei	Japon
Asia/Bishkek	Asia/Jayapura	Asia/Novokuznetsk	Asia/Tashkent	Mideast/Riyadh87
Asia/Brunei	Asia/Jerusalem	Asia/Novosibirsk	Asia/Tbilisi	Mideast/Riyadh88
Asia/Choibalsan	Asia/Kabul	Asia/Omsk	Asia/Tehran	Mideast/Riyadh89
Asia/Chongqing	Asia/Kamchatka	Asia/Oral	Asia/Tel_Aviv	PRC
Asia/Chungking	Asia/Karachi	Asia/Phnom_Penh	Asia/Thimbu	ROC
Asia/Colombo	Asia/Kashgar	Asia/Pontianak	Asia/Thimphu	ROK

Asia/Dacca	Asia/Kathmandu	Asia/Pyongyang	Asia/Tokyo	Singapore
Asia/Damascus	Asia/Katmandu	Asia/Qatar	Asia/Ujung_Pandang	Turkey

Paramètres de fuseaux horaires de la zone Océanie

REMARQUE : Les fuseaux horaires doivent être saisis exactement tels qu'ils s'affichent.

Le tableau suivant fournit les paramètres des fuseaux horaires de la zone Océanie pris en charge par le module Onboard Administrator.

Atlantic/Azores	Australia/Melbourne	Kwajalein	Pacific/Marquesas
Atlantic/Bermuda	Australia/North	NZ	Pacific/Midway
Atlantic/Canary	Australia/NSW	NZ-CHAT	Pacific/Nauru
Atlantic/Cape_Verde	Australia/Perth	Pacific/Apia	Pacific/Niue
Atlantic/Faeroe	Australia/Queensland	Pacific/Auckland	Pacific/Norfolk
Atlantic/Jan_Mayen	Australia/South	Pacific/Chatham	Pacific/Noumea
Atlantic/Madeira	Australia/Sydney	Pacific/Chuuk	Pacific/Pago_Pago
Atlantic/Reykjavik	Australia/Tasmania	Pacific/Easter	Pacific/Palau
Atlantic/South_Georgia	Australia/Victoria	Pacific/Efate	Pacific/Pitcairn
Atlantic/St_Helena	Australia/West	Pacific/Enderbury	Pacific/Pohnpei
Atlantic/Stanley	Australia/Yancowinna	Pacific/Fakaofo	Pacific/Ponape
Australia/ACT	Iceland	Pacific/Fiji	Pacific/Port_Moresby
Australia/Adelaide	Indian/Antananarivo	Pacific/Funafuti	Pacific/Rarotonga
Australia/Brisbane	Indian/Chagos	Pacific/Galapagos	Pacific/Saipan
Australia/Broken_Hill	Indian/Christmas	Pacific/Gambier	Pacific/Samoa
Australia/Canberra	Indian/Cocos	Pacific/Guadalcanal	Pacific/Tahiti
Australia/Currie	Indian/Comoro	Pacific/Guam	Pacific/Tarawa
Australia/Darwin	Indian/Kerguelen	Pacific/Honolulu	Pacific/Tongatapu
Australia/Eucla	Indian/Mahe	Pacific/Johnston	Pacific/Truk
Australia/Hobart	Indian/Maldives	Pacific/Kiritimati	Pacific/Wake
Australia/LHI	Indian/Mauritius	Pacific/Kosrae	Pacific/Wallis
Australia/Lindeman	Indian/Mayotte	Pacific/Kwajalein	Pacific/Yap
Australia/Lord_Howe	Indian/Reunion	Pacific/Majuro	US/Hawaii
—	—	—	US/Samoa

Paramètres de fuseaux horaires de la zone Europe

REMARQUE : Les fuseaux horaires doivent être saisis exactement tels qu'ils s'affichent.

Le tableau suivant fournit les paramètres des fuseaux horaires de la zone européenne pris en charge par le module Onboard Administrator.

Eire	Europe/Kaliningrad	Europe/Sarajevo
Europe/Amsterdam	Europe/Kiev	Europe/Simferopol
Europe/Andorra	Europe/Lisbon	Europe/Skopje
Europe/Athens	Europe/Ljubljana	Europe/Sofia
Europe/Belfast	Europe/London	Europe/Stockholm
Europe/Belgrade	Europe/Luxembourg	Europe/Tallinn
Europe/Berlin	Europe/Madrid	Europe/Tirane
Europe/Bratislava	Europe/Malta	Europe/Tiraspol
Europe/Brussels	Europe/Mariehamn	Europe/Uzhgorod
Europe/Bucharest	Europe/Minsk	Europe/Vaduz
Europe/Budapest	Europe/Monaco	Europe/Vatican
Europe/Busingen	Europe/Moscow	Europe/Vienna
Europe/Chisinau	Europe/Nicosia	Europe/Vilnius
Europe/Copenhagen	Europe/Oslo	Europe/Volgograd
Europe/Dublin	Europe/Paris	Europe/Warsaw
Europe/Gibraltar	Europe/Podgorica	Europe/Zagreb
Europe/Guernsey	Europe/Prague	Europe/Zaporozhye
Europe/Helsinki	Europe/Riga	Europe/Zurich
Europe/Isle_of_Man	Europe/Rome	GB
Europe/Istanbul	Europe/Samara	GB-Eire
Europe/Jersey	Europe/San_Marino	Poland
—	—	Portugal

Paramètres de fuseaux horaires de la zone polaire

REMARQUE : Les fuseaux horaires doivent être saisis exactement tels qu'ils s'affichent.

Le tableau suivant fournit les paramètres de fuseaux horaires de la zone polaire pris en charge par le module Onboard Administrator.

Antarctica/Casey	Antarctica/Mawson	Antarctica/South_Pole
Antarctica/Davis	Antarctica/McMurdo	Antarctica/Syowa

Antarctica/DumontDUrville	Antarctica/Palmer	Antarctica/Vostok
Antarctica/Macquarie	Antarctica/Rothera	Arctic/Longyearbyen

15 Assistance et autres ressources

Avant de contacter HP

Avant d'appeler HP, munissez-vous des informations suivantes :

- Journal de système d'intégrité actif (serveurs HP ProLiant Gen8 ou produits ultérieurs)

  Téléchargez et munissez-vous d'un journal d'intégrité du système couvrant les 7 jours précédant la détection de la panne. Pour plus d'informations, consultez le *Manuel de l'utilisateur de HP iLO 4* ou le *Manuel de l'utilisateur de HP Intelligent Provisioning* sur le site Web HP (http://www.hp.com/go/ilo/docs).

- Rapport SHOW ALL (Afficher tout) du module Onboard Administrator (pour les produits HP BladeSystem uniquement)

  Pour plus d'informations sur l'obtention du journal Onboard Administrator SHOW ALL, consultez le site Web de HP (http://www.hp.com/go/OAlog).

- Numéro d'enregistrement auprès de l'assistance technique (le cas échéant)
- Numéro de série du produit
- Nom et numéro du modèle de produit
- Numéro d'identification du produit
- Messages d'erreur obtenus, le cas échéant
- Cartes ou matériels complémentaires
- Matériel ou logiciel de fabricants tiers
- Type du système d'exploitation et niveau de révision

Informations de contact HP

Pour connaître les informations de contact aux États-Unis et dans le monde, consultez le site Web HP (http://www.hp.com/go/assistance).

Aux États-Unis :

- Pour contacter HP par téléphone, composez le 1 800-334-5144. Vos appels peuvent faire l'objet d'un enregistrement ou d'un contrôle, et ce, dans le but d'améliorer en permanence la qualité du service.
- Si vous avez acheté le service Care Pack (mise à niveau), consultez le site Web Support & Drivers (Assistance et drivers) (http://www8.hp.com/us/en/support-drivers.html). Si le site Web ne vous aide pas à résoudre le problème, composez le 1 800-633-3600. Pour plus d'informations sur les services Care Pack, consultez le site Web HP (http://pro-aq-sama.houston.hp.com/services/cache/10950-0-0-225-121.html).

Informations complémentaires

Pour ce qui suit...	Consulter...
Documentation de HP Onboard Administrator, y compris notes de version et manuels de l'utilisateur	Bibliothèque d'informations de HP Onboard Administrator (http://www.hp.com/support/oa/docs)
Documentation des boîtiers HP BladeSystem c3000/c7000	Bibliothèque d'informations de HP BladeSystem (http://www.hp.com/support/BladeSystem/docs)
HP Scripting Tools pour applets de commande Windows PowerShell OA	Outils de génération de scripts HP pour la bibliothèque d'informations PowerShell (http://www.hp.com/go/powershell/docs)
Informations sur le produit HP Onboard Administrator et ressources supplémentaires, notamment liens vers QuickSpecs, manuels de l'utilisateur, notes de version, livres blancs et autres documents	Site Web du produit HP Onboard Administrator (http://www.hp.com/go/oa)
Documentation HP Insight Management	Bibliothèque d'informations de HP Insight Management (http://www.hp.com/go/insightmanagement/docs)
Documentation iLO Management Engine	Bibliothèque d'informations de HP iLO Management Engine (http://www.hp.com/go/ilomgmtengine/docs)
Documentation HP Insight Remote Support	Bibliothèque d'informations de HP Insight Remote Support (http://www.hp.com/go/insightremotesupport/docs)

16 Acronymes et abréviations

CA

Certificate Authority (Autorité de certification)

CRL

Certificate Revocation List (Liste de révocation de certificats)

CSR

Certificate Signing Request (Demande de signature de certificat)

DC

Domain Controller (Contrôleur de domaine)

DCC

Device Control Channel (Canal de contrôle de périphérique)

DHCP

Dynamic Host Configuration Protocol (Protocole de configuration de serveur dynamique)

DN

Nom distinct

DNS

DNS

EBIPA

Enclosure Bay IP Addressing (Adressage IP des baies de boîtiers)

EDPC

Enclosure Dynamic Power Capping (Plafond d'alimentation dynamique du boîtier)

EEPROM

Electrical Erasable Programmable Read Only Memory (Mémoire en lecture seule effaçable électriquement)

EFM

Enclosure Firmware Management

ext2

Second Extended File System (Système de fichiers étendu)

FAT32

Table d'allocation de fichiers avec des valeurs de cluster représentées par des valeurs de 32 bits

FIPS

Federal Information Processing Standard (Norme de traitement des informations fédérales)

FQDN

Fully Qualified Domain Name (Nom de domaine pleinement qualifié)

FRU

Field Replaceable Unit (Unité remplaçable sur le terrain)

GC

Global Catalog (Catalogue global)

HPSC

HP Support Center

HTTPS

Hypertext Transfer Protocol Secure Sockets (Protocole de transfert des données sécurisées sur le Web)

I2C

Inter-Integrated Circuit (Circuit inter-intégré)

iLO

Integrated Lights-Out

KVM

Keyboard, Video and Mouse (clavier, vidéo et souris)

LDAP

Lightweight Directory Access Protocol

LOM

LAN on Motherboard (LAN sur carte mère)

MAC

Media Access Control

MMC

Microsoft Management Console

NTP

Network Time Protocol (Protocole d'heure réseau)

NVRAM

Mémoire non volatile

PCI

Payment Card Industry (Industrie de cartes de paiement)

PCIe

Peripheral Component Interconnect Express (Interconnexion de composants périphériques expresse)

PEM

Privacy Enhanced Mail (Courrier de confidentialité améliorée).

PIC

Peripheral Interface Controller (Contrôleur d'interface périphérique)

PIN

Numéro d'identification personnel

PKCS

Public-Key Cryptography Standards (Normes de cryptographie à clé publique)

PXE

Preboot Execution Environment (Environnement d'exécution de pré-démarrage)

RBSU

ROM-Based Setup Utility (Utilitaire de configuration basé sur la mémoire morte)

RIBCL

Remote Insight Board Command Language (Langage de commande de la carte Remote Insight)

RPM

Red Hat Package Manager

RSA

Clé de codage public Rivest, Shamir et Adelman

SAM

Security Account Manager (Gestionnaire de compte de sécurité)

SAS

Serial Attached SCSI

SLAAC

Stateless Address Autoconfiguration (Configuration automatique d'adresse sans état)

SOAP

Simple Object Access Protocol (Protocole simplifié d'accès aux objets)

SSH

Secure Shell

SSL

Secure Sockets Layer (Protocole de sécurisation des échanges sur l'Internet)

SUV

Serial, USB, Video (Série, USB, vidéo)

TFA

Two-Factor Authentication (Authentification à deux facteurs)

TFTP

Trivial File Transfer Protocol

TLS

Transport Layer Security (Protocole TLS)

TPM

Trusted Platform Module (Module de plate-forme sécurisée)

UEFI

Unified Extensible Firmware Interface (Interface extensible unifiée du microprogramme)

UID

Unit Identification (Identification d'unité)

VC

Virtual Connect

VCM

Virtual Connect Manager

VLAN

Virtual Local-Area Network (Réseau local virtuel)

VM

Virtual Machine (Machine virtuelle)

VSP

Virtual Serial Port (Port série virtuel)

17 Commentaires sur la documentation

HP s'engage à fournir une documentation qui répond à vos besoins. Pour nous aider à améliorer la documentation, envoyez les erreurs éventuelles, vos suggestions ou des commentaires (mailto:docsfeedback@hp.com). Incluez le titre et la référence du document, le numéro de version ou l'URL lors de la soumission de vos commentaires.

Index

A

Accès ad-hoc, DVD 175
Accès au module Onboard Administrator
  Connexion à l'interface du module Onboard Administrator 9
  Exigences d'accès 3
Accès au Web, activation 136
Accès des adresses IP, restriction 136
Accès réseau, configuration
  Accès réseau 136
  Écran Onboard Administrator Network Settings 78
  Onglet Login Banner 141
Actif à Standby 160
Activation IPv6 129
Active Health System 182
Active Onboard Administrator, écran 207
Administration des certificats 215
Administration SSH 348
Adressage EBIPA pour IPv4 150
Adressage EBIPA pour IPv6 153
Adresse de passerelle
  Adressage EBIPA pour IPv4 150
  Adressage EBIPA pour IPv6 153
  Adressage IP des baies de boîtiers 64
  Écran Onboard Administrator Network Settings 78
  Onglet IPv4 Settings 126
  Onglet IPv6 Settings 129
  Paramètres TCP/IP pour module OA en Standby, vu du module OA actif 230
Adresse DHCPv6 211
Adresses IP fiables 136
Adresse statique IPv6
  Écran Onboard Administrator Network Settings 78
  Écran TCP/IP Settings du module Onboard Administrator actif 211
  Onglet IPv6 Settings 129
Affectation des broches 358
Ajout d'un groupe d'annuaires
  Ajout d'un groupe LDAP 342
  Création de groupes d'annuaire 400
Ajout d'utilisateur
  Écran Local User Accounts 63
  Utilisateurs locaux 328
Ajout de réseau VLAN 179
Alertes
  Erreur de panne de périphérique 48
  Erreurs d'alimentation 47
  Erreurs d'emplacement 47
  Erreurs de configuration 47
  Erreurs de refroidissement 47
  Erreurs du module Insight Display 46
Alertes critiques 46
Alertes de précaution 46
AlertMail 117
Algorithmes de code d'authentification de message SSH 17
Alimentation, erreurs 47
Alimentation, état
  Écran Power Subsystem 316
  Informations d'alimentation 317
Alimentations 316
Alimentation secteur redondante, perte
  Gestion de l'alimentation 301
Alimentation secteur redondante, sélection 301
Alimentation virtuelle 249
Annonces de routeur
  Écran Onboard Administrator Network Settings 78
  Onglet IPv6 Settings 129
Annulation de l'inscription à HP Insight Remote Support 183
Aperçu du rack 102
Application d'un cryptage robuste
  Accès réseau 136
  FIPS 56
  Fonctionnalités de sécurité cryptographique et valeurs par défaut 17
  Onglet FIPS 139
Architecture de réseau BladeSystem 15
Assistance technique
  Assistance et autres ressources 440
  Avant de contacter HP 440
  Informations de contact HP 440
Assistant d'installation, utilisation
  Assistant First Time Setup 54
  Exécution de l'assistant d'installation 12
Authentification à deux facteurs
  Authentification à deux facteurs 350
  Création d'autorités de certification et configuration de l'autorisation à deux facteurs pour comptes de groupe LDAP et d'utilisateur local 404
  Création d'autorités de certification subordonnées 410
  Création d'une autorité de certification racine 408
  Installation de la chaîne d'autorités de certification pour authentification à deux facteurs 421

Authentification à deux facteurs, activation
Activation de l'authentification à deux facteurs 426
Two-Factor Authentication (Authentification à deux facteurs) 350
Authentification à deux facteurs, avec LDAP 427
Authentification à deux facteurs, certificats de serveur 410
Authentification à deux facteurs, certificats utilisateur
Authentification à deux facteurs 350
Fourniture d'informations de certificat utilisateur x509 413
Installation de certificats utilisateur sur le compte administrateur local 424
Modification des informations de certificat des utilisateurs locaux 333
Onglet Certificate Information de l'authentification à deux facteurs 351
Onglet Certificate Upload de l'authentification à deux facteurs 351
Signature de la CSR d'utilisateur avec la clé level1CA 413
Stockage d'un certificat utilisateur sur une carte à puce ou un navigateur 417
Vérification de certificats 416
Authentification à deux facteurs, configuration avec comptes d'utilisateur local 419
Authentification à deux facteurs, configuration de comptes de groupe LDAP et d'utilisateur local 404
Authentification à deux facteurs, configuration de répertoires pour certificats 407
Authentification à deux facteurs, connexion à l'interface utilisateur OA 427
Authentification à deux facteurs, création d'une clé d'utilisateur 412
Authentification à deux facteurs, délai d'expiration de session 420
Authentification à deux facteurs, exemples de configuration d'interface CLI 430
Authentification à deux facteurs, infrastructure à clé publique 404
Authentification à deux facteurs, plan de récupération 419
Authentification à deux facteurs, plus d'informations sur les autorités de certification et certificats 432
Authentification à deux facteurs, présentation 404
Authentification à deux facteurs, stockage de certificats 417
Authentification à deux facteurs, vérification de certificats
Problèmes connus divers 393
Vérification de certificats 416
Authentification à deux facteurs avec LDAP, résolution des problèmes 429
Authentification d'utilisateurs 7
Authentification des utilisateurs, menu 326
Authentification LDAP, activation
Écran Directory Settings 75, 334
Authentification LDAP+TFA 427
Authentification TFA+LDAP 427

B

Baie d'interconnexion
Baies d'interconnexion 291
Écran Interconnect Bay 293
Baie d'interconnexion, boutons virtuels 298
Baie d'interconnexion, informations d'état 296
Baie d'interconnexion, informations de l'URL de gestion 291
Baie d'interconnexion, mappage de ports 298
Baie d'interconnexion, menu UID State 291
Baie d'interconnexion, menu Virtual Power 291
Baie d'interconnexion, résumé 291
Baie de périphérique, écran d'aperçu 237
Baie de périphérique, onglet d'état
Onglet Device Bay Status 240
Onglet Server Blade Information 246
Baie de serveur, informations 240
Baies d'interconnexion, séquence d'alimentation 123
Baies de périphérique
Baies de périphérique 237
Baies de périphérique, séquence d'alimentation 120
Bannière de connexion
Accès réseau 136
Onglet Login Banner 141
Basculement, forcer 160
Basculement sur perte de liaison 141
Bloc d'alimentation redondant, sélection
Écran Power Management 86
Gestion de l'alimentation 301
Boîtier, boutons virtuels 113
Boîtier, configuration 112
Boîtier, gestion
Gestion de boîtiers 206
Présentation du module Onboard Administrator 4
Boîtier, liaison 206
Boîtier, mise hors tension 206
Boîtier, paramètres
Écran Enclosure Information 113
Écran Rack and Enclosure Settings 60
Paramètres du boîtier 113
Boîtier, sélection
Écran Enclosure Selection 58
Sélection de boîtiers 113
Boîtiers multiples, gestion 207

Boutons virtuels
Boutons virtuels de la baie d'interconnexion 298
Écran Enclosure Information 113
Onglet de périphériques virtuels de lame d'extension E/S 290
Onglet Server Blade Virtual Devices 249
Onglet Virtual Buttons du module Onboard Administrator actif 209
Onglet Virtual Buttons du module Onboard Administrator en mode Standby 229
Boutons virtuels, baie d'interconnexion 298
Boutons virtuels, baie de serveur 249
Boutons virtuels, boîtier 113
Boutons virtuels, Onboard Administrator
Onglet Virtual Buttons du module Onboard Administrator actif 209
Onglet Virtual Buttons du module Onboard Administrator en mode Standby 229

C

CA (autorité de certification) 396
CA (autorité de certification), installation pour authentification à deux facteurs 421
Câblage 23
Câblage, module Onboard Administrator 23
Certificat, demande
Onglet Certificate Request 217
Onglet Standby Certificate Request 234
Certificat d'annuaire, informations 337
Certificat d'annuaire, téléchargement 338
Certificate Request, onglet 217
Chiffrements
Fonctionnalités de sécurité cryptographique et valeurs par défaut 17
Onglet FIPS 139
Chiffrements de sécurité 139
Chiffrement SSH 17
Clé SSH, algorithmes d'échange 17
Clé USB, prise en charge
Baies de périphérique 237
Lecteur de DVD 160
Mise à jour du microprogramme 221
CLI (interface de ligne de commande) 356
Compatible iLO Federation 254
Composants, identification 3
Composants Insight Display
Composants de l'écran Insight Display 2 pouces du modèle HP BladeSystem c7000 26
Composants de l'écran Insight Display 3 pouces des modèles HP BladeSystem c3000 et c7000 27
Comptes d'utilisateurs locaux, activation
Écran Directory Settings 75, 334
Comptes utilisateur 7
Comptes utilisateur locaux
Écran Local User Accounts 63
Utilisateurs locaux 328
Compte utilisateur, ajout
Écran Local User Accounts 63
Utilisateurs locaux 328
Compte utilisateur, modification 63
Compte utilisateur, suppression
Écran Local User Accounts 63
Utilisateurs locaux 328
Configuration, erreurs 47
Configuration, modification de boîtier et de périphérique 14
Configuration du compte administrateur 62
Connecteur série 358
Connexion à l'annuaire, test 401
Connexion au module Onboard Administrator 9
Connexion DVD
Baies de périphérique 237
Onglet Server Blade Virtual Devices 249
Consignation de système distant
Journal système 227
Onglet Log Options 227
Console de gestion, interconnexions
Écran Interconnect Bay 293
Écran Interconnect Bay Summary 291
Console de gestion, supervision distante iLO 254
Contacter HP
Avant de contacter HP 440
Informations de contact HP 440
Cryptage robuste
FIPS 56
Fonctionnalités de sécurité cryptographique et valeurs par défaut 17
Onglet FIPS 139
CSR, champ d'objet 428
CSR, génération
Création de clés d'utilisateur et de CSR 412
Génération d'une CSR et d'une nouvelle clé de serveur 411
Current Default Gateway
Écran TCP/IP Settings du module Onboard Administrator actif 211
Paramètres TCP/IP pour module OA en Standby, vu du module OA actif 230

D

Date et heure 123
Détection manuelle
Détection manuelle 202
Enclosure Firmware Management 195

Initiation d'une mise à jour ou détection manuelle 276
Microprogramme 274
Diagnostics des problèmes 366
DNS dynamique
Écran Onboard Administrator Network Settings 78
Onglet IPv4 Settings 126
Onglet IPv6 Settings 129
Onglet NIC Options 135
Paramètres TCP/IP du boîtier 126
Documentation
Informations complémentaires 441
Dynamic Host Configuration Protocol (DHCP)
Écran Onboard Administrator Network Settings 78
Écran TCP/IP Settings du module Onboard Administrator actif 211
Onglet IPv4 Settings 126
Onglet IPv6 Settings 129
Paramètres TCP/IP pour module OA en Standby, vu du module OA actif 230
Dynamic Power
Écran Power Management 86
Exécution de l'installation du module Insight Display 29
Gestion de l'alimentation 301

E

EBIPA, baie de serveur 64
EBIPA, instructions de configuration
Adressage IP des baies de boîtiers 64, 147
EBIPA, paramètres 64
EBIPA (Enclosure Bay IP Addressing) 147
Échec de connexion, après redémarrage
Onglet Trusted Hosts 137
Problèmes connus divers 393
Échecs d'événement 203
Écran Blade and Port Info 38
Écran Chat Mode 42
Écran Enclosure Info 39
Écran Enclosure Settings 38
Écran KVM Menu 46
Écran Power and Thermal 300
Écran SNMP Settings 142
Écran USB Key Menu 43
Erreur de génération CSR 393
Erreurs, panne de périphérique 48
Erreurs, ventilateur 47
Erreurs d'alimentation 47
Erreurs d'emplacement 47
Erreurs d'installation 47
Erreurs de configuration 47
Erreurs de refroidissement 47
Erreurs de ventilateur 47
Erreurs du module Insight Display 46
Erreurs Onboard Administrator 366
État de lame d'extension E/S 289
État du ventilateur 320
Étendu, journal système 227
Événements de service Insight Remote Support 190
Exigences, accès 3
Exigences, Onboard Administrator 3

F

Fichier de configuration OpenSSL 408
Fichiers de script 59
Fonctionnalités Enclosure KVM 49
Fuseaux horaires de la zone Afrique 433
Fuseaux horaires de la zone Amérique 434
Fuseaux horaires de la zone Asie 436
Fuseaux horaires de la zone Europe 438
Fuseaux horaires de la zone polaire 438
Fuseaux horaires de zone Océanie 437
Fuseaux horaires universels 433

G

Gestion de l'alimentation
Écran Enclosure Power Meter 310
Écran Power Management 86
Gestion de l'alimentation 301
Gestion de l'alimentation de boîtier 300
Gestion de l'alimentation, planification 300
Gestion de la configuration 59
Gestion des microprogrammes du boîtier
Enclosure Firmware Management 195
Microprogramme 274
Gestion des utilisateurs 326
Gestion des ventilateurs
Gestion des ventilateurs et de la ventilation 318
Sous-système thermique 320
Gestion du module Onboard Administrator, présentation 4
Groupe d'annuaires, ajout
Ajout d'un groupe LDAP 342
Création de groupes d'annuaire 400
Groupe d'annuaires, paramètres
Ajout d'un groupe LDAP 342
Écran Directory Group Configuration 73
Groupes d'annuaires 341
Modification d'un groupe LDAP 345
Groupe LDAP, ajout 342
Groupe LDAP, modification 345
Groupes LDAP, imbriqués
Écran Directory Group Configuration 73
Écran Directory Settings 75, 334
Groupes d'annuaires 341

H

HP, site Web 440
HP BladeSystem Insight Display 26
HP BladeSystem Insight Display, accès 28

HP BladeSystem Insight Display, composants de l'écran
Composants de l'écran Insight Display 2 pouces du modèle HP BladeSystem c7000 26
Composants de l'écran Insight Display 3 pouces des modèles HP BladeSystem c3000 et c7000 27
HP BladeSystem Insight Display, configuration du boîtier 29
HP BladeSystem Insight Display, écran Blade and Port Info 39
HP BladeSystem Insight Display, écran Chat Mode 42
HP BladeSystem Insight Display, écran Enclosure Info 39
HP BladeSystem Insight Display, écran Enclosure Settings 38
HP BladeSystem Insight Display, écran KVM Menu 46
HP BladeSystem Insight Display, écran View User Note 42
HP BladeSystem Insight Display, erreurs
Erreur de panne de périphérique 48
Erreurs d'alimentation 47
Erreurs d'emplacement 47
Erreurs de configuration 47
Erreurs de refroidissement 47
Erreurs du module Insight Display 46
HP BladeSystem Insight Display, menu principal 35
HP BladeSystem Insight Display, menu USB Key 43
HP BladeSystem Insight Display, navigation 35
HP BladeSystem Insight Display, option Health Summary 37
HP BladeSystem Insight Display, option Turn Enclosure UID On/Off 41

I

Icônes 204
Icônes d'état 204
Identification d'unité (UID), voyants 46
iLO, informations sur le processeur 254
iLO, supervision distante 254
Image ISO
Baies de périphérique 237
Enclosure Firmware Management 195
Lecteur de DVD 160
IML (journal de maintenance intégré) 253
Informations d'état, alimentation 317
Informations d'état, lame d'extension E/S 289
Informations d'état, mise à jour de microprogramme 204
Informations d'état, Onboard Administrator
Écran Active Onboard Administrator 207
Écran Standby Onboard Administrator 228
Informations d'état, ventilateurs 320
Informations d'état du boîtier
Connexion à l'interface du module Onboard Administrator 9
Écran Enclosure Information 113
Informations de contact HP 440
Informations de lame d'extension E/S 291
Informations récapitulatives des microprogrammes 108
Informations sur la carte réseau 246
Informations sur le serveur 246
Inscription à Insight Remote Support 183
Insight Display
Accès à l'écran HP BladeSystem c3000 Insight Display 28
HP BladeSystem Insight Display 26
Insight Display 353
Présentation du module Insight Display 27
Insight Display, accès 28
Insight Display, écran Blade or Port Info 39
Insight Display, écran Chat Mode 42
Insight Display, écran Enclosure Info 39
Insight Display, écran Enclosure Settings
Écran Enclosure Settings 38
Exécution de l'installation du module Insight Display 29
Insight Display, écran Health Summary 37
Insight Display, écran KVM Menu 46
Insight Display, écran Turn Enclosure UID On/Off 41
Insight Display, écran USB Key Menu 43
Insight Display, écran View User Note 42
Insight Display, navigation 35
Installation, erreurs 47
Installation de DVD-ROM 163
Installation de modules 23
Installation de modules de supervision de boîtier 23
Installation de modules Onboard Administrator 23
Integrated Remote Console (IRC) 393
Intégration de HP SSO 349
Interface CLI, accès refusé 393
Interface de ligne de commande, utilisation 356
Interfaces 6
IPv6, activation
Écran Onboard Administrator Network Settings 78
Onglet IPv6 Settings 129

J

Journal Enclosure Firmware Management
Journal Enclosure Firmware Management 203
Journaux de gestion des microprogrammes 280
Journal système
Journal système 227

Journal système pour module Onboard Administrator en Standby 236
Onglet Log Options 227
Journal système étendu 227
Journaux des événements
Collectes de données Insight Remote Support 192
Événements de service Insight Remote Support 190

K
KVM, utilisation
Fonctionnalités 49
Onglet USB du module Onboard Administrator actif 210

L
Lame de serveur, informations d'état
Onglet d'informations de lame d'extension E/S 291
Onglet Server Blade Information 246
Lame de serveur, informations FRU 246
lame de serveur, partenaire 365
Lame de serveur, périphériques virtuels 249
Lame de serveur, réinitialisation de l'alimentation 237
Lame de stockage 284
Langue d'affichage 55
LDAP, authentification et contrôle d'accès
Activation de l'authentification de services d'annuaire LDAP auprès de Microsoft Active Directory 396
Authentification TFA+LDAP 427
Services de certificat 396
Lecteur CD-ROM
Installation et configuration interactives du lecteur de DVD/CD-ROM 163
Lecteur de DVD 160
Lecteur de DVD
Installation et configuration interactives du lecteur de DVD/CD-ROM 163
Lecteur de DVD 160
Onglet Server Blade Virtual Devices 249
Liaison de boîtiers 206

M
Mappage de ports 256
Mappage de ports, baie d'interconnexion 298
Mappage de ports, lame de serveur
Modification de mappage de ports pour lames de serveur HP Integrity i2 365
Tableau de mappage de ports de baie de périphérique pour boîtier c3000 262
Vue graphique de mappage de ports de baie de périphérique pour boîtier c3000 258
Vue graphique de mappage de ports de baie de périphérique pour boîtier c7000 266
Mappage de ports, lame de serveur double densité
Tableau de mappage de ports de baie de périphérique pour boîtier c3000 262
Vue graphique de mappage de ports de baie de périphérique pour boîtier c3000 258
Vue graphique de mappage de ports de baie de périphérique pour boîtier c7000 266
Mappage de ports, vue graphique
Vue graphique de mappage de ports de baie de périphérique pour boîtier c3000 258
Vue graphique de mappage de ports de baie de périphérique pour boîtier c7000 266
Mappage de ports Telco AMC
Tableau de mappage de ports de baie de périphérique pour boîtier c3000 262
Tableau de mappage de ports de baie de périphérique pour boîtier c7000 271
Masque de sous-réseau 230
Messages d'erreur 366
Microprogramme, mise à niveau inférieure 221
Mise à jour du microprogramme 221
Mise à jour manuelle
Détection manuelle 202
Enclosure Firmware Management 195
Initiation d'une mise à jour ou détection manuelle 276
Microprogramme 274
Mise à jour manuelle 203
Mise hors tension 206
Mode d'amorçage 246
Mode FIPS, activation
FIPS 56
Fonctionnalités de sécurité cryptographique et valeurs par défaut 17
Onglet FIPS 139
Mode FIPS, paramètres par défaut 17
Modes de topologie 104
Modification de paramètres, boîtier 14
Modification de réseau VLAN 179
Module de langue 225
Module Onboard Administrator 23
Module Onboard Administrator, première exécution 8
Module Onboard Administrator, présentation 1
Module Onboard Administrator, redondance 1

Module Onboard Administrator en mode Standby
Écran Standby Onboard Administrator 228
Module Onboard Administrator en mode Standby 228
Module Onboard Administrator en mode Standby, onglet Certificate Request 234
Module Onboard Administrator en mode Standby, onglet Certificate Upload 236
Mot de passe robuste
FIPS 56
Fonctionnalités de sécurité cryptographique et valeurs par défaut 17
Onglet FIPS 139
Paramètres de mot de passe 333

N
Navigateur, dépannage 390
Navigateur, exigences
Exigences d'accès 3
Problèmes connus liés au navigateur 390
Navigation 96
Navigation dans l'arborescence
Arborescence 96
Modification de vue d'arborescence et de vue graphique pour lames de serveur HP Integrity i2 363
Navigation dans l'interface 96
Navigation graphique 99
Niveaux de privilège
Ajout d'un groupe LDAP 342
Modification d'un groupe LDAP 345
Modification de l'utilisateur local 330
Nom du module Onboard Administrator 230
Note de l'utilisateur, écran 42
Numéros de téléphone 440
Assistance et autres ressources 440
Informations de contact HP 440

O
Onboard Administrator, interfaces 6
Onboard Administrator, navigation 96
One Time Boot
Baies de périphérique 237
Onglet Boot Options 251
Onglet Anonymous Data 138
Onglet d'options de consignation 227
Onglet Firmware Summary 274
Onglet Graphical
Graphical View 311
Onglet IPv4 Settings
Onglet IPv4 Settings 126
Paramètres TCP/IP du boîtier 126
Onglet IPv6 Settings
Accès réseau 136
Link Loss Failover 141
Onglet Advanced Settings 135
Onglet IPv6 Settings 129
Onglet NIC Options 135
Onglet Language Pack du module Onboard Administrator actif 225
Onglet NIC Options 135
Onglet Trusted Hosts
Accès réseau 136
Onglet Trusted Hosts 137
Onglet Virtual Buttons du module Onboard Administrator actif 209
Options de gestion de l'alimentation 86
Options de session
Configuration de l'expiration de la session Onboard Administrator 420
Onglet Session Options 352

P
Paramètres, carte réseau 230
Paramètres, mot de passe 333
Paramètres d'annuaire
Écran Directory Settings 75, 334
Préparation de l'annuaire 396
Paramètres d'expiration de session
Configuration de l'expiration de la session Onboard Administrator 420
Onglet Session Options 352
Paramètres de codage 17
Paramètres de courrier d'alerte 117
Paramètres de mot de passe 333
Paramètres de sécurité
Fonctionnalités de sécurité cryptographique et valeurs par défaut 17
Onglet FIPS 139
Paramètres de sécurité avancés 139
Paramètres de test d'annuaire 339
Paramètres du boîtier 113
Écran Enclosure Information 113
Paramètres du boîtier 113
Paramètres du rack 60
Paramètres IP, boîtier 126
Paramètres NIC
Onglet IPv4 Settings 126
Onglet NIC Options 135
Paramètres TCP/IP du boîtier 126
Paramètres TCP/IP pour module OA en Standby, vu du module OA actif 230
Paramètres réseau 78
Paramètres SNMP
Écran Enclosure SNMP Settings 85
Paramètres SNMP 142
Paramètres TCP/IP
Écran Onboard Administrator Network Settings 78
Écran TCP/IP Settings du module Onboard Administrator actif 211
Onglet IPv4 Settings 126
Paramètres TCP/IP du boîtier 126
Paramètres TCP/IP pour module OA en Standby, vu du module OA actif 230

Paramètres TCP/IP, accessibles à partir du module Onboard Administrator en Standby 230
Paramètres TCP/IP du module Onboard Administrator actif 211
Paramètres utilisateur 330
Passerelle par défaut 211
Périphériques, erreurs 48
Périphériques, USB 210
Périphériques virtuels
Lecteur de DVD 160
Onglet Server Blade Virtual Devices 249
Perte de liaison 141
Plafond de puissance
Écran Power and Thermal 300
Gestion de l'alimentation 301
Planification de la gestion de l'alimentation 300
Plafond dynamique de boîtier 300
Port de maintenance, câblage 358
Port série 358
Précautions 46
Préférences de l'utilisateur 55
Présentation 1
Prise en charge de lien FQDN
Baies de périphérique 237
Écran iLO 254
Écran Interconnect Bay 293
Écran Interconnect Bay Summary 291
Écran Rack Overview 102
Virtual Connect Manager 353
Prise en charge de Linux 356
Prise en charge du boîtier par iLO Federation, activation 136
Prise en charge iLO Federation, boîtier 136
Problèmes, diagnostics 366
Problèmes connus
Problèmes connus divers 393
Problèmes connus liés au navigateur 390
Problèmes de réseau connus 392
Problèmes de réseau 392
Protocoles cryptographiques
Fonctionnalités de sécurité cryptographique et valeurs par défaut 17
Onglet FIPS 139
Protocoles de sécurité
Fonctionnalités de sécurité cryptographique et valeurs par défaut 17
Onglet FIPS 139

R

Rack, résumé de microprogramme 108
Récupération du mot de passe, administrateur 14
Récupération flash d'urgence 11
Redondance 1
Redondance d'alimentation, perte
Écran Power Management 86
Gestion de l'alimentation 301
Réinitialisation iLO 237
Remote Support, annulation de l'inscription 183
Remote Support, chargement d'un certificat 194
Remote Support, collecte de données
Collectes de données Insight Remote Support 192
Inscription à Insight Remote Support 183
Remote Support, conditions requises 183
Remote Support, événements 190
Remote Support, informations de certificat 193
Remote Support, inscription 183
Résolution des problèmes 366
Résolution des problèmes d'utilitaire de mise à jour de microprogramme 366
Ressources d'aide
Informations de contact HP 440
Utilisation de l'aide en ligne 13
Restrictions de protocole 136
Résumé des périphériques 157
Revendeur agréé
Assistance et autres ressources 440
Informations de contact HP 440
Rôles utilisateur 7

S

Script de configuration, utilisation
Scripts de configuration 359
Utilisation de scripts de configuration 359
Secure Boot 246
Secure Boot, exigences de gestion de microprogramme
Baies de périphérique 237
Enclosure Firmware Management 195
Initiation d'une mise à jour ou détection manuelle 276
Microprogramme 274
Onglet Boot Options 251
Séquence d'alimentation, baies d'interconnexion 123
Séquence d'alimentation, baies de périphérique 120
Serveur, options de démarrage 251
Serveur DNS 230
Services de certificat, présentation 396
Services de détection d'emplacements
Connexion à l'interface du module Onboard Administrator 9
Écran Enclosure Information 113
Écran Rack Firmware 108
Écran Rack Overview 102
Onglet Rack Topology 105
Site Web HP 440
Source de mise à jour de microprogramme 221
Sous-système de ventilateurs, état 320
SSH, activation 136
SSO 349
Standby à Actif 236

Suppression d'un compte utilisateur
Écran Local User Accounts 63
Utilisateurs locaux 328
Système d'exploitation, déploiement sans assistance 169

T

TCP/IP (Transmission Control Protocol/Internet Protocol) 230
Téléchargement de certificat
Installation de la chaîne d'autorités de certification pour authentification à deux facteurs 421
Téléchargement d'un certificat 337
Téléchargement du certificat de contrôleur de domaine (facultatif) 397
Téléchargement de fichiers 440
Telnet, activation 136
Test, consignation distante 227
Test, services d'annuaire 339
Test de connexion à l'annuaire 401
Test de consignation distante 227
Test de courrier d'alerte 117
Test de groupe LDAP 339
Topologie du rack, onglet 105
Transmission Control Protocol/ Internet Protocol (TCP/IP) 230

U

UEFI, mode d'amorçage 246
UID, voyant 46
UID de boîtier, basculement 113
UID de lame de serveur, basculement 237
UID de module Onboard Administrator, basculement 229
Utilisateur local, ajout
Ajout d'un utilisateur local 329
Utilisateurs locaux 328
Utilisateur local, modification
Modification de l'utilisateur local 330
Utilisateurs locaux 328
Utilisateurs connectés 351
Utilisation de l'aide 13
Utilitaire de mise à jour de microprogramme, résolution des problèmes 366

V

Valeurs usine par défaut, réinitialisation 361
Ventilation, erreurs 47
Version du microprogramme, affichage
Affichage des versions des microprogrammes 282
Écran Rack Firmware 108
Enclosure Firmware Management 195
Versions de microprogrammes, variations 284
Version SSH, prise en charge 348
Versions SSL, prise en charge 348
Virtual Connect Manager
Onglet IPv4 Settings 126
Paramètres TCP/IP du boîtier 126
Virtual Connect Manager 353
Virtual media, résolution des problèmes 393
VLAN, configuration
Ajout, édition et suppression de réseaux VLAN 179
Configuration VLAN 175
Paramètres VLAN 177
Vue du rack
Écran Rack Overview 102
Vue du rack 102
Vue graphique 363